

<<IDA Pro权威指南 (第2版)>>

图书基本信息

书名：<<IDA Pro权威指南 (第2版)>>

13位ISBN编号：9787115273680

10位ISBN编号：7115273685

出版时间：2012-2

出版时间：人民邮电

作者：Chris Eagle

页数：493

译者：石华耀,段桂菊

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<IDA Pro权威指南 (第2版) >>

### 内容概要

《IDA Pro权威指南(第2版)》共分为六部分，首先介绍了反汇编与逆向工程的基本信息和IDA Pro的背景知识，接着讨论了IDA Pro的基本用法和高级用法，然后讲解了其高扩展性及其在安全领域的实际应用，最后介绍了IDA的内置调试器(包括Bochs调试器)，一方面让用户对IDA Pro有全面深入的了解，另一方面让读者掌握IDA Pro在现实中的应用。相比上一版，这一版以IDA6.0为基础，介绍了它的新的、基于Qt的图形用户界面，以及IDAPython插件。

《IDA Pro权威指南(第2版)》适合IT领域的所有安全工作者阅读。

## <<IDA Pro权威指南 (第2版)>>

### 作者简介

Chris

Eagle是美国加利福尼亚州蒙特雷海军研究生院计算机科学系高级讲师。

他设计了很多IDA插件，还与人合著了Gray

Hat Hacking一书。

他应邀在Balckhat、Defcon、Toorcon和Shmoocon等众多安全会议上发表过演讲。

# <<IDA Pro权威指南 (第2版)>>

## 书籍目录

### 第一部分 IDA简介

#### 第1章 反汇编简介

- 1.1 反汇编理论
- 1.2 何为反汇编
- 1.3 为何反汇编
  - 1.3.1 分析恶意软件
  - 1.3.2 漏洞分析
  - 1.3.3 软件互操作性
  - 1.3.4 编译器验证
  - 1.3.5 显示调试信息
- 1.4 如何反汇编
  - 1.4.1 基本的反汇编算法
  - 1.4.2 线性扫描反汇编
  - 1.4.3 递归下降反汇编
- 1.5 小结

#### 第2章 逆向与反汇编工具

- 2.1 分类工具
  - 2.1.1 file
  - 2.1.2 PE Tools
  - 2.1.3 PEiD
- 2.2 摘要工具
  - 2.2.1 nm
  - 2.2.2 ldd
  - 2.2.3 objdump
  - 2.2.4 otool
  - 2.2.5 dumpbin
  - 2.2.6 c++filt
- 2.3 深度检测工具
  - 2.3.1 strings
  - 2.3.2 反汇编器
- 2.4 小结

#### 第3章 IDA Pro背景知识

- 3.1 Hex-Rays公司的反盗版策略
- 3.2 获取IDA Pro
  - 3.2.1 IDA版本
  - 3.2.2 IDA许可证
  - 3.2.3 购买IDA
  - 3.2.4 升级IDA
- 3.3 IDA支持资源
- 3.4 安装IDA
  - 3.4.1 Windows安装
  - 3.4.2 OS X和Linux安装
  - 3.4.3 IDA与SELinux

## <<IDA Pro权威指南 (第2版)>>

3.4.4 32位IDA与64位IDA

3.4.5 IDA目录的结构

3.5 IDA用户界面

3.6 小结

### 第二部分 IDA基本用法

#### 第4章 IDA入门

4.1 启动IDA

4.1.1 IDA文件加载

4.1.2 使用二进制文件加载器

4.2 IDA数据库文件

4.2.1 创建IDA数据库

4.2.2 关闭IDA数据库

4.2.3 重新打开数据库

4.3 IDA桌面简介

4.4 初始分析时的桌面行为

4.5 IDA桌面提示和技巧

4.6 报告bug

4.7 小结

#### 第5章 IDA数据显示窗口

5.1 IDA主要的数据显示窗口

5.1.1 反汇编窗口

5.1.2 函数窗口

5.1.3 输出窗口

5.2 次要的IDA显示窗口

5.2.1 十六进制窗口

5.2.2 导出窗口

5.2.3 导入窗口

5.2.4 结构体窗口

5.2.5 枚举窗口

5.3 其他IDA显示窗口

5.3.1 Strings 窗口

5.3.2 Names 窗口

5.3.3 段窗口

5.3.4 签名窗口

5.3.5 类型库窗口

5.3.6 函数调用窗口

5.3.7 问题窗口

5.4 小结

#### 第6章 反汇编导航

6.1 基本IDA导航

6.1.1 双击导航

6.1.2 跳转到地址

6.1.3 导航历史记录

6.2 栈帧

6.2.1 调用约定

## <<IDA Pro权威指南 (第2版)>>

- 6.2.2 局部变量布局
- 6.2.3 栈帧示例
- 6.2.4 IDA栈视图
- 6.3 搜索数据库
  - 6.3.1 文本搜索
  - 6.3.2 二进制搜索
- 6.4 小结

### 第7章 反汇编操作

- 7.1 名称与命名
  - 7.1.1 参数和局部变量
  - 7.1.2 已命名的位置
  - 7.1.3 寄存器名称
- 7.2 IDA中的注释
  - 7.2.1 常规注释
  - 7.2.2 可重复注释
  - 7.2.3 在前注释和在后注释
  - 7.2.4 函数注释
- 7.3 基本代码转换
  - 7.3.1 代码显示选项
  - 7.3.2 格式化指令操作数
  - 7.3.3 操纵函数
  - 7.3.4 数据与代码互相转换
- 7.4 基本数据转换
  - 7.4.1 指定数据大小
  - 7.4.2 处理字符串
  - 7.4.3 指定数组
- 7.5 小结

### 第8章 数据类型与数据结构

- 8.1 识别数据结构的用法
  - 8.1.1 数组成员访问
  - 8.1.2 结构体成员访问
- 8.2 创建IDA结构体
  - 8.2.1 创建一个新的结构体(或联合)
  - 8.2.2 编辑结构体成员
  - 8.2.3 用栈帧作为专用结构体
- 8.3 使用结构体模板
- 8.4 导入新的结构体
  - 8.4.1 解析C结构体声明
  - 8.4.2 解析C头文件
- 8.5 使用标准结构体
- 8.6 IDA TIL文件
  - 8.6.1 加载新的TIL文件
  - 8.6.2 共享TIL文件
- 8.7 C++逆向工程基础
  - 8.7.1 this指针

## <<IDA Pro权威指南 (第2版)>>

- 8.7.2 虚函数和虚表
- 8.7.3 对象生命周期
- 8.7.4 名称改编
- 8.7.5 运行时类型识别
- 8.7.6 继承关系
- 8.7.7 C++逆向工程参考文献
- 8.8 小结

### 第9章 交叉引用与绘图功能

- 9.1 交叉引用
  - 9.1.1 代码交叉引用
  - 9.1.2 数据交叉引用
  - 9.1.3 交叉引用列表
  - 9.1.4 函数调用
- 9.2 IDA绘图
  - 9.2.1 IDA外部(第三方)图形
  - 9.2.2 IDA的集成绘图视图
- 9.3 小结

### 第10章 IDA的多种面孔

- 10.1 控制台模式IDA
  - 10.1.1 控制台模式的共同特性
  - 10.1.2 Windows控制台
  - 10.1.3 Linux控制台
  - 10.1.4 OS X控制台
- 10.2 使用IDA的批量模式
- 10.3 小结

### 第三部分 IDA高级应用

#### 第11章 定制IDA

- 11.1 配置文件
  - 11.1.1 主配置文件: ida.cfg
  - 11.1.2 GUI配置文件: idagui.cfg
  - 11.1.3 控制台配置文件: idatui.cfg
- 11.2 其他IDA配置选项
  - 11.2.1 IDA颜色
  - 11.2.2 定制IDA工具栏
- 11.3 小结

#### 第12章 使用FLIRT签名来识别库

- 12.1 快速库识别和鉴定技术
- 12.2 应用FLIRT签名
- 12.3 创建FLIRT签名文件
  - 12.3.1 创建签名概述
  - 12.3.2 识别和获取静态库
  - 12.3.3 创建模式文件
  - 12.3.4 创建签名文件
  - 12.3.5 启动签名

## &lt;&lt;IDA Pro权威指南 (第2版)&gt;&gt;

## 12.4 小结

## 第13章 扩展IDA的知识

## 13.1 扩充函数信息

## 13.1.1 IDS文件

## 13.1.2 创建IDS文件

## 13.2 使用loadint扩充预定义注释

## 13.3 小结

## 第14章 修补二进制文件及其他IDA限制

## 14.1 隐藏的补丁程序菜单

## 14.1.1 更改数据库字节

## 14.1.2 更改数据库中的字

## 14.1.3 使用汇编对话框

## 14.2 IDA输出文件与补丁生成

## 14.2.1 IDA生成的MAP文件

## 14.2.2 IDA生成的ASM文件

## 14.2.3 IDA生成的INC文件

## 14.2.4 IDA生成的LST文件

## 14.2.5 IDA生成的EXE文件

## 14.2.6 IDA生成的DIF文件

## 14.2.7 IDA生成的HTML文件

## 14.3 小结

## 第四部分 扩展IDA的功能

## 第15章 编写IDA脚本

## 15.1 执行脚本的基础知识

## 15.2 IDC语言

## 15.2.1 IDC变量

## 15.2.2 IDC表达式

## 15.2.3 IDC语句

## 15.2.4 IDC函数

## 15.2.5 IDC对象

## 15.2.6 IDC程序

## 15.2.7 IDC错误处理

## 15.2.8 IDC永久数据存储

## 15.3 关联IDC脚本与热键

## 15.4 有用的IDC函数

## 15.4.1 读取和修改数据的函数

## 15.4.2 用户交互函数

## 15.4.3 字符串操纵函数

## 15.4.4 文件输入/输出函数

## 15.4.5 操纵数据库名称

## 15.4.6 处理函数的函数

## 15.4.7 代码交叉引用函数

## 15.4.8 数据交叉引用函数

## 15.4.9 数据库操纵函数

## 15.4.10 数据库搜索函数



## &lt;&lt;IDA Pro权威指南 (第2版)&gt;&gt;

- 15.4.11 反汇编行组件
- 15.5 IDC脚本示例
  - 15.5.1 枚举函数
  - 15.5.2 枚举指令
  - 15.5.3 枚举交叉引用
  - 15.5.4 枚举导出的函数
  - 15.5.5 查找和标记函数参数
  - 15.5.6 模拟汇编语言行为
- 15.6 IDAPython
- 15.7 IDAPython脚本示例
  - 15.7.1 枚举函数
  - 15.7.2 枚举指令
  - 15.7.3 枚举交叉引用
  - 15.7.4 枚举导出的函数
- 15.8 小结

## 第16章 IDA软件开发工具包

- 16.1 SDK简介
  - 16.1.1 安装SDK
  - 16.1.2 SDK的布局
  - 16.1.3 配置构建环境
- 16.2 IDA应用编程接口
  - 16.2.1 头文件概述
  - 16.2.2 网络节点
  - 16.2.3 有用的SDK数据类型
  - 16.2.4 常用的SDK函数
  - 16.2.5 IDA API迭代技巧
- 16.3 小结

## 第17章 IDA插件体系结构

- 17.1 编写插件
  - 17.1.1 插件生命周期
  - 17.1.2 插件初始化
  - 17.1.3 事件通知
  - 17.1.4 插件执行
- 17.2 构建插件
- 17.3 插件安装
- 17.4 插件配置
- 17.5 扩展IDC
- 17.6 插件用户界面选项
  - 17.6.1 使用SDK的“选择器”对话框
  - 17.6.2 使用SDK创建自定义表单
  - 17.6.3 仅用于Windows的用户界面生成技巧
  - 17.6.4 使用Qt生成用户界面
- 17.7 脚本化插件
- 17.8 小结

## &lt;&lt;IDA Pro权威指南 (第2版)&gt;&gt;

## 第18章 二进制文件与IDA加载器模块

- 18.1 未知文件分析
- 18.2 手动加载一个Windows PE文件
- 18.3 IDA加载器模块
- 18.4 使用SDK编写IDA加载器
  - 18.4.1 “傻瓜式”加载器
  - 18.4.2 构建IDA加载器模块
  - 18.4.3 IDA pcap加载器
- 18.5 其他加载器策略
- 18.6 编写脚本化加载器
- 18.7 小结

## 第19章 IDA处理器模块

- 19.1 Python字节码
- 19.2 Python解释器
- 19.3 使用SDK编写处理器模块
  - 19.3.1 processor\_t结构体
  - 19.3.2 LPH 结构体的基本初始化
  - 19.3.3 分析器
  - 19.3.4 模拟器
  - 19.3.5 输出器
  - 19.3.6 处理器通知
  - 19.3.7 其他processor\_t成员
- 19.4 构建处理器模块
- 19.5 定制现有的处理器
- 19.6 处理器模块体系结构
- 19.7 编写处理器模块
- 19.8 小结

## 第五部分 实际应用

## 第20章 编译器变体

- 20.1 跳转表与分支语句
- 20.2 RTTI实现
- 20.3 定位main函数
- 20.4 调试版与发行版二进制文件
- 20.5 其他调用约定
- 20.6 小结

## 第21章 模糊代码分析

- 21.1 反静态分析技巧
  - 21.1.1 反汇编去同步
  - 21.1.2 动态计算目标地址
  - 21.1.3 导入的函数模糊
  - 21.1.4 有针对性地攻击分析工具
- 21.2 反动态分析技巧
  - 21.2.1 检测虚拟化
  - 21.2.2 检测“检测工具”
  - 21.2.3 检测调试器

## &lt;&lt;IDA Pro权威指南 (第2版)&gt;&gt;

- 21.2.4 防止调试
- 21.3 使用IDA对二进制文件进行“静态去模糊”
  - 21.3.1 面向脚本的去模糊
  - 21.3.2 面向模拟的去模糊
- 21.4 基于虚拟机的模糊
- 21.5 小结
  
- 第22章 漏洞分析
  - 22.1 使用IDA发现新的漏洞
  - 22.2 使用IDA在事后发现漏洞
  - 22.3 IDA与破解程序开发过程
    - 22.3.1 栈帧细目
    - 22.3.2 定位指令序列
    - 22.3.3 查找有用的虚拟地址
  - 22.4 分析shellcode
  - 22.5 小结
  
- 第23章 实用IDA插件
  - 23.1 Hex-Rays
  - 23.2 IDAPython
  - 23.3 collabREate
  - 23.4 ida-x86emu
  - 23.5 Class Informer
  - 23.6 MyNav
  - 23.7 IdaPdf
  - 23.8 小结
- 第六部分 IDA调试器
- 第24章 IDA调试器
  - 24.1 启动调试器
  - 24.2 调试器的基本显示
  - 24.3 进程控制
    - 24.3.1 断点
    - 24.3.2 跟踪
    - 24.3.3 栈跟踪
    - 24.3.4 监视
  - 24.4 调试器任务自动化
    - 24.4.1 为调试器操作编写脚本
    - 24.4.2 使用IDA插件实现调试器操作自动化
  - 24.5 小结
  
- 第25章 反汇编器/调试器集成
  - 25.1 背景知识
  - 25.2 IDA数据库与IDA调试器
  - 25.3 调试模糊代码
    - 25.3.1 启动进程
    - 25.3.2 简单的解密和解压循环
    - 25.3.3 导入表重建

## <<IDA Pro权威指南 (第2版)>>

25.3.4 隐藏调试器

25.4 IDAStealth

25.5 处理异常

25.6 小结

### 第26章 其他调试功能

26.1 使用IDA进行远程调试

26.1.1 使用Hex-Rays调试服务器

26.1.2 连接到远程进程

26.1.3 远程调试期间的异常处理

26.1.4 在远程调试过程中使用脚本和插件

26.2 使用Bochs进行调试

26.2.1 Bochs IDB模式

26.2.2 Bochs PE模式

26.2.3 Bochs磁盘映像模式

26.3 Appcall

26.4 小结

附录A 使用IDA免费版本5.0

附录B IDC/SDK交叉引用

## 章节摘录

版权页：插图：在这个例子中，我们应用了libc、libcrypto、libkrb5、libresolv及其他库的签名。

有时候，我们根据二进制文件中的字符串来选择签名。

其他情况下，我们选择与二进制文件中已经确定的其他库关系密切的签名。

最终，导航窗口会在导航带的中间显示一个深色的代码带，在导航带的最左边缘显示一个更小的深色代码带。

要确定二进制文件中剩下的非库代码的性质，你需要进行更加深入的分析。

在这个例子中，我们知道，中间的深色代码带是一种尚未识别的库，而左侧的深色代码带则为应用程序代码。

12.3创建FLIRT签名文件 如前所述，IDA不可能自带现有的每一个静态库的签名文件。

为了向IDA用户提供创建他们自己的签名所需的工具和信息，Hex—Rays开发了FLAIR（Fast Library Acquisition for Identification and Recognition，快速获取库的识别和鉴定）工具集，你可以从IDA发行版光盘上获得FLAIR工具，被授权用户也可以从Hex—Rays网站上下载该工具。

与IDA的另外几个附加件一样，FLAIR工具通过一个Zip文件发布。

Hex—Rays不一定会为每一个版本的IDA发布新版的FLAIR工具，因此，只需使用最新版本的FLAIR工具，只要它不高于你的IDA版本即可。

安装FLAIR实用工具的过程非常简单，只需解压相关的Zip文件即可。

尽管如此，我们仍然强烈建议你创建一个专用的flair目录作为目标目录，因为zip文件可能并不包含一个顶级目录。

解压FLMR文件后，你会发现几个文本文件，它们是FLAIR工具的文档资料。

其中特别有用的文件如下所示。

readme.txt。

这个文件总体概述签名创建过程。

plb.txt。

这个文件描述静态库解析器plb.exe的用法。

库解析器将在12.3.3节中详细讨论。

pat.txt。

这个文件详细说明了模式文件的格式，它是签名创建过程的第一步。

我们还将在12.3.3节介绍模式文件。

sigmake.txt。

这个文件描述sigmake.exe文件的用法，该文件用于从模式文件生成.sig文件。

请参阅12.3.4节了解详情。

其他顶级目录包括bin目录，其中包括FLAIR工具的所有可执行文件和startup目录，后者包含与各种编译器及其相关的输出文件类型（PE、ELF等）有关的常见启动顺序的模式文件。

对于6.1之前的版本，FLAIR工具只能在Windows命令提示符下运行，但其生成的签名文件可以用在所有的IDA版本中（Windows、Linux和OSX）。

<<IDA Pro权威指南 (第2版) >>

编辑推荐

《IDA Pro权威指南(第2版)》适合IT领域的所有安全工作者阅读。

<<IDA Pro权威指南（第2版）>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>