<<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

<<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。

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

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 Identificationand 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FLA瓜工具，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FLAJR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）。

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。

版权说明