<<黑客调试技术揭秘>>

图书基本信息

书名：<<黑客调试技术揭秘>>

13位ISBN编号：9787121028021

10位ISBN编号：7121028026

出版时间：2006-7

出版时间：电子工业出版社

作者：卡斯帕克尔

页数：516

字数：548000

译者：周长发

<<黑客调试技术揭秘>>

内容概要

本书是帮助应用程序员和系统程序员理解调试过程的指南，揭示了各种调试器的实用使用技巧，说明了如何操作调试器以及如何克服障碍和修复调试器，介绍了黑客利用调试器和反汇编器来寻找程序弱点和实施攻击的方法。
通过本书，程序员将学会如何弄清楚计算机系统内部的结构、如何重建没有提供源程序的程序的运行算法、如何修改程序以及如何调试驱动程序。
本书还详细介绍了在Windows和UNIX操作系统中调试应用程序和驱动程序的方法。
对于各种调试技术，书中都给出了带有详尽解释的源代码。
如果你是具有C/C++或者Pascal/Delphi语言实际编程经验的程序员，那么本书就是使你的技术升华至一个新的台阶的宝典。

作者简介

Kris Kaspersky是一位技术作家。
他是《黑客反汇编技术揭秘》、《代码优化：有效使用内存》和《CD破解揭秘：防止未经许可的CD拷贝的保护技术》等书籍，以及大量涉及破解、反汇编和代码优化文章的作者。
他解决了许多与安全和系统编程有关的问题，包括编译器的开发、优化技术、

<<黑客调试技术揭秘>>

书籍目录

章节摘录

主操作系统成了寄宿操作系统的基础。
这个“旅店”的一个房间必须分配为隔离区。
我们都知道，当安装一个新程序时，操作系统经常会出现问题，这可能是因为没有正确地使用安装程序、函数库之间存在冲突、广告软件或者只是因为偶然因素(比如因果报应)。
只要能从其他渠道获得程序，就尽可能地不使用从不可靠的渠道获得的程序，这种做法是很明智的。
只需在仿真器中分配一个单独的虚拟机，这类程序就不能摆脱虚拟机！
3.5.2 管理员使用的仿真器 从管理员的观点来看，仿真器主要是各种不同试验的测试区域：
安装几十个不同的UNIX变体，并彻底地测试它们。
安装一个系统，删除它，然后再重新安装，稍微修改一下其配置。
为了获得一份工作，你不仅要有文凭，是你所工作的领域的一个专家，而且还必须具有实际工作经验。
对于数据恢复方面的工作来说，也是如此。
如果没有进行特殊的准备工作，并不推荐你在你的主操作系统中运行Disk Editor (对于Disk Doctor来说，更是如此)。
这是因为，不能保证这类工具能够修正磁盘错误，而不会弄坏你的磁盘。
简单地说，仿真器是很好的测试区域，这在过去是难以成真的美梦。
在大型机构中，管理员通常都有镜像服务器，所有的补丁程序都首先会在镜像服务器中进行测试。
小型机构难以负担用于这种目的的额外机器。
在这种情形中，仿真器就可以大展身手。
此外，仿真器还可用于测试各种不同的试验程序。
如果证实了程序的弱点，就可以采取紧急措施来改正它。
虚拟机与主操作系统和其他虚拟机之间的交互一般通过LAN(也是虚拟的)来进行。
假定你的计算机有512 MB～1024.MB的RAM，就可以通过结构化查询语言(sQL)和Web服务器、一个“隔离带”、一个防火墙和几个工作站来创建一个内部网模型(如图3.9所示)。
这个测试完全适合于在一台家用计算机中进行。
换句话说，对于测试目的来说，仿真器比任何东西都适合。
在仿真器中，你既可以攻击，也可以管理网络。
3.5.3软件开发人员使用的仿真器 驱动程序开发人员是最喜爱仿真器的人群。
内核不仅不会自行修正错误，还会报复性地破坏整个硬盘，使得多年积累的数据毁于一旦而不可恢复。
对于驱动程序开发人员来说，就像铁道工习惯于火车轮子的咔嗒声，频繁地重新启动和死机是司空见惯的。
另外，大多数内核级调试器都要求两台通过LAN或者至少调制解调器相连在一起的计算机。
当然，从专业开发人员的观点来看，使用两台计算机并不是过分奢侈。
然而，你如何摆放它们呢?不断地左右转动脑袋并不是一件舒服的事情。
有时，这就像要将你的脑袋从脖子上拧下来一样!

版权说明