黑客札记

必备的核心安全信息来源

Windows 安全手册

- 保护Windows 2000 Server，Windows XP和Windows Server 2003的安全
- 掌握黑客寻觅、探测和攻破Windows系统的途径
- 学习使用免费的和Windows系统内置的安全工具

Michael O'Dea 著

石朝江 汪青青 译

清华大学出版社

黑客札记

Windows安全手册

Michael O'Dea 著
石朝江 汪青青 译

清华大学出版社
北京

Michael O'Dea
Hacknotes Windows Security Portable Reference
EISBN：0-07-222785-0

图书在版编目(CIP)数据

黑客札记：Windows 安全手册/欧迪尔(O'Dea, M.)著；石朝江，汪青青译. —北京：清华大学出版社，2005.5
书名原文：Hacknotes Windows Security Portable Reference
ISBN 7-302-10744-0

Ⅰ. W…　Ⅱ. ①欧… ②石… ③汪…　Ⅲ. 窗口软件，Windows—安全技术—技术手册　Ⅳ. TP316.7-62

中国版本图书馆 CIP 数据核字(2005)第 027342 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
责任编辑：常晓波
印 刷 者：北京市清华园胶印厂
装 订 者：三河市金元装订厂
发 行 者：新华书店总店北京发行所
开　　本：150×230　**印张**：18.25　**字数**：278 千字
版　　次：2005 年 5 月第 1 版　2005 年 5 月第1 次印刷
书　　号：ISBN 7-302-10744-0/TP·7155
印　　数：1～3000
定　　价：35.00 元

作者简介

Michael O'Dea 是信息安全公司 Foundstone 的产品服务项目经理。Michael 投身于信息技术已有 10 多年，研究的技术如企业数据加密、病毒防御、防火墙以及各种 UNIX/Windows 平台上的代理服务方案。目前，Michael 正在为 Foundstone 的企业级漏洞管理产品系列开发定制的集成方案。在加入 Foundstone 之前，Michael 作为资深分析师为 Disney Worldwide Services 公司的互联网安全部门工作过，该公司是 Walt Disney 公司的数据服务分支机构；Michael 还做过 Network Associates 公司的顾问，其间他参与出版了多本信息安全专著，其中包括 *Hacking Exposed: Fourth Edition*（即国内引进的著名的《黑客大曝光》）与 *Special Ops: Internal Network Security*。

技术编辑简介

Arne Vidstrom 是瑞典国防研究所的 IT 安全研究科学家。在成为电信巨头 Telia 的一名计算机安全工程师之前，Arne 做过渗透测试、源代码安全评审、安全配置测试，及安全配置清单的构建。Arne 获得了电子工程专业的大学文凭，他还获得了 Karlstad 大学的数学专业学士学位。Arne 还用业余时间搭建了一个 Windows 安全方面的网站 ntsecurity.nu，他在该站点发布自己开发的免费安全工具以及发现的漏洞。

致谢

本书要献给很多人。首先，作者想感谢自己的家人与朋友，感谢他们的不断支持与鼓励，没有这些也不可能出版本书。

在信息安全领域，任何人都不会是孤立的；而是通过团队协作才会发现最佳的解决方案。同样，作者也想感谢自己的所有同事，多年来正是他们的想法与引导才使得本书能够成形，这些人包括Foundstone的工作人员（排名不分先后）——Steve Andrés、Brian Kenyon、John Bock、Dave Cole、Stuart McClure、Robin Keir、Mike Barry、Joe Wu、Chris Moore、Erik Birkholz、Marshall Beddoe，以及其他很多曾不时提出宝贵意见与教导过作者的人。

这里要特别感谢Arne Vidström，正是因为他在技术编辑上的突出贡献才保证了本书的精确性与完整性。最后要强调的是，感谢McGraw-Hill/Osborne的编辑人员，他们包括：一直忍耐无穷无尽问题的Jane Brownlow，保持项目进度的Athena Honore，做了极多编辑工作的Andrea Bouchard与Jennifer Malnick（他们让人误以为本书写得好是作者的功劳）。

《黑客札记》丛书

McGraw-Hill/Osborne 为安全专业人士策划了一套全新的便携手册。这套速成书籍对页数进行了控制，使之成为真正的便携手册。

《黑客札记》丛书的目标是：

- 提供易懂易用、精简的安全参考资讯。
- 教导大家如何保护网络或系统，展现黑客与犯罪分子如何利用知名手段闯入系统，阐述防御黑客攻击的最佳方式。
- 本套丛书能让那些新接触安全主题的人很快地上手，并且能提供精练、直接的知识源泉。为此大家会发现自己会不时地要参考本书。

这套丛书设计得便于携带，放在书包里也不会增加太多份量，并且使用时也不会引起不必要的注意。这套丛书尽可能地利用图表、表格与项目列表，只有在理解重点必须用到屏幕截图时，才会使用图例。更为重要的是，这套便携且轻巧的参考书不会用无关的空话烦人，也就不会让大家在繁忙工作之余还要费劲啃它们；我们保持了书写的清楚、精练与中肯。

不管是信息安全领域的新手(希望不用翻查 400 余页资料就能得到有用的基础知识与基本事实)，还是了解手册使用价值(手册相当于另一个大脑，它含有丰富的有用清单、表格及快速确认时所需的特定细节；或者说手册相当于一部安全话题的便携参考)的老练的专业人士，《黑客札记》丛书都能对你有所帮助。

丛书中的关键元素及图标

我们尽可能有条理地组织、展现本书。本书使用紧凑的形式，

另外还放入页标签来标记主题。本书最后的“参考中心”包含了大家希望快速、容易访问到的信息及表格。

图标说明

本书中用到的图标使得导航非常容易。每种黑客技术或攻击都用一个特殊的利剑图标突出标示。

这种图标代表一种黑客技术或攻击

获得黑客用以闯入脆弱系统的各种技术/谋略的详细信息。

只要可能，每种黑客技术或攻击也会有一种防御手段；防御手段同样也有自己的特殊图标——盾牌。

这种图标代表对抗黑客技术/攻击的防御手段

获得如何防御所展现黑客技术或攻击的精练细节。

《黑客札记》丛书设计时还用到了其他特殊元素，其中有一些脱离于正文的信息小块，这是为了引起注意。

“i”图标代表一种信息提示，表明阅读该具体小节内容时应该记住这一点。

这种火焰图标代表一种热门事物或一个重要问题，要避免花样繁多的缺陷，就不应该忽视它们。

命令与代码清单

本书通篇都用黑体字显示用户命令输入以表强调，比如：

```
[bash] # whoami
root
```

简介

Windows 家族的操作系统自诩是目前市场上对用户最具友好性的管理控制工具。工作站、服务器这两个版本的操作系统都有着一致且直观的界面，这让用户觉得自己不需什么帮助就能顺利完成一些复杂的事务，如设置 Web 服务、远程管理或文件共享等。这种特征已经成为 Windows 操作系统风行的基础。而且这也是 Windows 安全记录的基础。

在 Windows Server 2003 之前，默认安装后的 Microsoft Windows 家族成员很少利用甚至完全不用大量的安全控制，尽管这些控制能将系统被攻破的风险减至最小。虽然这些扩展的选项让那些对安全性比较敏感的管理员能利用强大的安全工具，但操作系统最初的安全配置却对攻击者大开方便之门。由于让应用程序或服务器正常工作时并不一定要配置安全参数，于是人们常常就忽视或遗忘了巩固系统，这就是一条经典规则的影响——“没被破坏的时候就不用修补它”。

《黑客札记》丛书之《Windows 安全手册》的目的是帮助 Windows 管理员理解那些用来寻找、定性及攻击 Windows 操作系统时所用的工具及技术；有助于避免这些攻击的操作系统自带的功能及实用程序；部署这些功能及实用程序的方法。这些内容的最终目标就是慢慢让人们理解 Windows 安全的始末，并不是只了解某个具体的漏洞可被利用，而是要学习出现漏洞后“如何研究”它们。

本书的组织形式

尽管本书适合作为参考材料，但我们还是按一种适合通览的方

式组织了内容。在第一部分中，我们讨论了黑客与安全的基本知识、枚举与收集信息的基本技术。在本书中，我们不但给出了扫描技术及探测技术背后的概念，而且还展现了自己尝试这些方法时用到的工具以及第一手的黑客经验。

在第二部分中，我们考察了一些常见的攻击，包括针对核心Windows身份验证功能的攻击以及针对最著名Windows目标——Internet信息服务(IIS)的攻击。在这一部分中，我们探讨了Windows身份验证及常见服务中的弱点，讨论了如何巩固系统且限制弱点的暴露。第7章在谈到攻击IIS时，我们甚至还逐步展现了如何利用Internet上的免费代码，通过已知漏洞攻破系统。

最后，在第三部分与第四部分中，我们谈到了Windows操作系统中的安全工具与子系统，利用它们能帮助管理员保护自身环境，不管是内部台式机的联网环境，还是Internet上的Web服务器群。我们讨论了各种防御技术，从文件系统、本地系统安全策略这类最基本的技术，直至更复杂的活动目录域级别的安全技术(用到了组策略、网络流量部署与文件系统加密)。

本书最后的“参考中心”列出了书中讨论的所有概念及工具。“参考中心”给出了一组随时会用到的表格，其中的信息从TCP/IP数据类型直至有用的Windows安全工具、命令行语法。

如何阅读本书

本书每一章都可以当作一个独立的部分来读，可以不分先后。每章阐述概念与技术的时候都经过了大量思考与关注，使得各章行文清楚、精练；另外每章还提供了指向本书别处相关信息的交叉引用。这种方式可以让我们从一开始就比较容易消化信息，并且使以后的引用更容易。

除了极少数的例外，每章开始都讨论了该章主题涉及的概念与术语。解释了背景知识之后，接着介绍了与该主题相关的所有工具及Windows功能。在一些较为复杂的章节中，比如处理网络与文件系统加密的那几章，我们还给出了逐步利用所讨论技术的完整步骤。

目录

第一部分　网络安全原理和方法

参考中心

第一部分

网络安全原理和方法

第1章

追踪：了解攻击目标

内容提要

- 追踪
- 小结