
Mc Graw Hill Education
安氏推荐 iS-One
网络安全机密与解决方案
Network Security Secrets & Solutions
HACKING EXPOSED
“任何一位 Windows 管理员都不应该错过的珍宝。”
—— Todd Sabin，著名安全程序员，不可或缺的pwdump2工具的开发者
「Windows 2000」
黑客大曝光
【美】Joel Scambray,Stuart McClure 著
杨洪涛 译
Mc Graw Hill
清华大学出版社

Windows 2000 黑客大曝光

——网络安全机密与解决方案

【美】 Joel Scambray , Stuart McClure 著

杨洪涛 译

清华大学出版社

（京）新登字158号

北京市版权局著作权合同登记号 01-2002-3395

EISBN 0-07-219262-3

内容提要

本书是《黑客大曝光》畅销书系列中的一本，主要针对Windows 2000操作系统，从攻击者和防御者的不同角度系统阐述了计算机和网络的入侵手段及相应防御措施。本书内容包括：网络和系统安全的概念及Windows 2000的安全体系；网络中发现和探测目标的技术和防御方法；入侵和占领整个系统、扩展权限、清除作案痕迹的方法以及相应的防御措施；IIS5，SQL Server，终端服务器，Internet客户端的攻击技术以及物理攻击、拒绝服务攻击；Windows 2000的安全工具。

全书注重案例分析，讲解了很多具体攻击的过程，更重要的是对几乎所有讨论过的攻击手段都提供了相应的对策。

本书是安全漏洞的宝典，是负责安全保障工作的网络管理员和系统管理员的必读之书，也可作为信息管理员以及对计算机和网络安全感兴趣的人员的重要参考书。

书　名：Windows 2000黑客大曝光：网络安全机密与解决方案

作　者：Joel Scambray,Stuart McClure

译　者：杨洪涛

出版者：清华大学出版社（北京清华大学学研大厦，邮编100084）

印刷者：北京耀华印刷有限公司

发行者：新华书店总店北京发行所

开　本：异16　　印张：32.75　字数：626千字

版　次：2002年10月第1版　2002年10月第1次印刷

印　数：0001~6000

书　号：ISBN 7-302-05848-2/TP・3462

定　价：53.00元

黑暗中的眼睛

小榕

这是一本黑客技术手册，它的目标读者是网络管理人员，系统工程师，信息安全领域的技术人员和所有对黑客技术感兴趣的人。无论您是否已经精通黑客技术，我都建议您把本书通读一遍，因为在这里您一定会发现一些您以前所不了解的东西。

当前，Windows 2000 已经广泛使用，对 Windows 2000 攻击的手法和技巧也层出不穷。本书主要描述的是针对 Win2000 平台的黑客攻击技术，和以往介绍黑客技术的作品不同，本书并不是对每一种攻击技巧的简单罗列，而是对当前常见，有效的攻击手法进行深入地分析和解说。本书从内容上覆盖了网络安全基础知识、操作系统安全、Web 应用安全、高级攻击技术与防范措施等方面的知识。除此以外还提供了大量的实例，来提高可读性，并且还针对相应的手法对流行的工具进行了描述和介绍，深度和广度结合适当。

网络安全的重要性目前已经得到企业各方面人士的认可，对网管人员和系统工程师以及开发人员，网络安全技术已经是必不可少的技能要求之一，不懂得网络安全技术，或者不具备必要的网络安全知识、技能的网管人员和系统工程师，都是不合格的技术人员。

对于攻击者来说，书中提到的某些攻击技术无疑是他们所期待的，通过对本书的阅读他们能够丰富自己的攻击手段，了解更多的相关知识。

对于 Windows 2000 的系统管理员来说，本书的内容或许会让你惊出一身冷汗。因为你进入了一个你从来不曾了解的领域，在这个领域中，你会看到黑暗中窥视的眼睛。

只有进入黑暗，才能洞悉黑暗。

关于作者

Joel Scambray

Joel Scambray是国际畅销的Internet安全系列丛书《黑客大曝光》(http://www.hackingexposed.com)的作者之一。该书在2001年已出版了第3版。Joel多年的IT安全顾问经历成为他写作的主要来源。他的客户既包括“财富50强”中的企业，也有新成立的公司，从中他获得了关于各种安全技术的大量经过实际检验的知识，他曾经设计和分析过各种应用程序和产品的安全架构。Joel为多个组织提供Windows 2000安全咨询服务，包括计算机安全协会、MIS培训协会、SANS(系统管理、网络与安全协会)、ISSA(信息系统安全协会)、ISACA(信息系统审计与控制协会)和很多大型企业，他还一直担任Foundstone公司“Windows终极黑客”课程的主讲。现在他是Foundstone公司(http://www.foundstone.com)的高层管理人员，在此之前曾任Ernst & Young公司的经理、Infoworld公司的测试中心高级分析员和一家大型商业房地产公司的IT主管。Joel的学历背景包括加利福尼亚大学洛杉矶分校(UCLA)的高级学位，并且持有信息系统安全专家认证(CISSP)证书。

——Joel Scambray的联系方式：joel@hackingexposed.com

Stuart McClure

Stuart十余年的IT和安全工作经历为《黑客大曝光》系列带来了丰富的内容。他是这本书的创建者之一，并帮助推进本书成为国际上空前畅销的网络安全书籍。Stuart也是“安全观察”(http://www.infoworld.com/security)的合作创建者，这个每周专栏自1998年来曾多次提出重要的安全问题、漏洞和弱点。目前Stuart是一流的安全评估、咨询、培训和技术公司Foundstone的董事长、首席技术官。

在参与创建Foundstone之前，Stuart是Ernst & Young公司安全配置

服务组的高级经理，负责项目管理、攻击、入侵评审和技术鉴定。他曾经担任过的职位包括Inforworld测试中心的安全分析员，曾评估过近100个网络和安全产品，特别是防火墙、安全审核、入侵检测和公钥体系(PKI)产品。在进入Infoworld之前，Stuart曾在其他公司的IT部门任网络、系统和安全管理员，管理Novell、NT、Solaris、AIX和AS/400等平台超过6年之久。

Stuart持有科罗拉多玻尔大学的学士学位和多种认证证书，包括ISC2的CISSP(信息系统安全专家认证)、Novell的CNE(认证网络工程师)和Check Point的CCSE(认证安全管理员)。

——Stuart McClure的联系方式：stuart@hackingexposed.com

D

关于技术审阅者

Chip Andrews

Chip Andrews 是 Clarus 公司的软件安全设计师，有超过 12 年的软件开发经验。他为 *Microsoft Certified Professional* 和 *SQL Server Magazine* 等杂志撰写过关于 SQL 安全性和软件开发问题的文章。Chip 曾多次在与 Microsoft SQL Server 安全问题和安全应用程序设计有关的会议上发表演讲。

Erik Pace Birkholz, CISSP

Erik 是 Foundstone 的首席顾问。Erik 的主要研究领域是 Internet 和 Intranet 技术以及它们所包含的协议、网络设备和操作系统的安全问题。他主要关注攻击和渗透测试以及安全架构设计。

Erik 还是 Foundstone 公司的“终极黑客：动手做”和“终极 NT/2000 安全：动手做”课程的主讲。在加入 Foundstone 公司之前，他是 Internet 安全系统公司(ISS)的西海岸顾问组的评估主管。在 ISS 之前，Erik 为 Ernst & Young 公司的 eSecurity 服务部门工作。他是国家攻击和渗透小组的成员，“极端黑客”课程的讲师。Erik 还在国家计算机安全协会(NSCA)从事了两年的研究分析。

Erik 对国际畅销书《黑客大曝光》作出了重要的贡献，他的研究成果还发表在国家计算机安全协会期刊和 Foundstone 的“数字战场”上。他还在 Black Hat 简报和 Internet 安全会议(TISC)上报告了他的研究。

Erik 持有宾夕法尼亚 Dickinson 学院的学士学位，曾获 1999–2000 年度优秀毕业生奖“Metzger Conway Fellow”。他持有认证信息系统安全专家(CISSP)和 Microsoft 认证系统工程师(MCSE)证书。

Clinton Mugge

Clinton Mugge 是为 Foundstone 的客户提供信息安全咨询服务的首席管理顾问，专门负责网络评估、产品测试和安全架构。他持有认证信息系统安全专家(CISSP)证书。Mugge 有 7 年的安全工作经验，涉及物理安全、主机、网络架构和间谍事件调查。他曾与政府机构和众多 IT 公司进行过联合政府调查、突发事件响应项目和网络评估工作。在加入 Foundstone 之前，Mugge 为 Ernst & Young 公司工作，后来又任美国陆军反情报官员。Mugge 多次在会议上发表演讲、为专栏撰写文章，还是 Osborne/McGraw-Hill 出版的《突发事件响应》一书的技术评论。Mugge 持有计算机管理学士学位和市场营销学士学位。

——Clinton Mugge 的联系方式：clinton.mugge@foundstone.com

Eric Schultze

Eric Schultze 在过去的 9 年中一直从事信息技术和安全工作，大部分时间关注于评估和保护 Microsoft 技术和平台。他经常在信息会议上发表演讲，包括 NetWorld+Interop、Usenix、BlackHat、SANS 和 MIS，是计算机安全协会的教师。Schultze 还经常出现在电视和多种媒体上，包括 NBC、CNBC、TIME、ComputerWorld 和 The Standard。Schultze 曾为 Foundstone、SecurityFocus.com、Ernst & Young、Price Waterhouse、Bealls 和 Salomon Brothers 公司工作。他是《黑客大曝光》第一版的作者之一，目前是 Microsoft 公司的安全程序经理。

David Wong

David 是计算机安全专家，Foundstone 公司的首席顾问。他进行过大量的安全产品评测以及网络攻击和渗透测试。David 在进入 Foundstone 之前是大型电讯公司的软件工程师，负责开发进行网络侦察和监视的软件。

序

如果你是一位网络管理员，那么在你的网络中，很可能在某个地方存在安全漏洞。如果只有一个漏洞，那么情况还不糟糕。你只要找到并修复它就可以了。只要知道了具体的解决方案，你甚至都不用关心这个漏洞的细节。然而不幸的是，实际情况通常不会这么简单。在稍大一些的网络中，总会存在数百个不同严重程度的弱点，随着时间的推移，你还会不断地发现新的弱点。此时你应该怎么办？如何决定首先应该解决哪个问题呢？

惟一合理的方法，是理解这些弱点是什么，它们是如何被利用的，它们的影响是什么，有哪些防御方法等等。有了这些知识之后，你就能够明智地确定什么是你的网络中最严重的问题，以及如何去解决它们。

但是到哪里去寻找你需要的信息呢？这些信息在 Internet 上广泛传播，通过大量的 Web 站点、邮件列表、FTP 服务器、IRC 频道等等。完全凭借自己的能力去寻找这些信息是一项复杂的工作。幸运的是，你不需要这样做——提供这些信息正是本书的编写目的。本书含有关于 Windows 2000 安全的大量的知识。这些信息是作者多年积累下来的，在《黑客大曝光》丛书中公布出来。

本书继承了这个传统，但是重点集中于 Windows 2000 的安全话题。作者收集了大量关于威胁、攻击和防御的最新信息，并提出了他们自己的有深刻见解的分析。本书是任何一位 Windows 管理员都不应该错过的信息宝藏。

当然，攻击者也会利用这些信息作为攻击的指导。于是，有人提出发布这些信息会导致安全局势的恶化。保持这些信息的机密性，只让少数受到信任的人能够接触到它们，会更好一些。但是，这不但会让管理员们仍然蒙在鼓里，不能对安全问题做出明智决断，而且它假设地下计算机是不会自行发现或传播这些信息的。经验表明，这种假设是靠不住的。

在我写这个序言时，Internet 正在遭受第一波的“红码”(Code Red)蠕虫病毒。在短短的几天之内，数以百万计的 IIS 服务器被感染，并被作为蠕虫进一步扩展的基地。如果这第一次的感染还不够糟糕，可以预料的是病毒还会开始新一轮攻击，这次会更糟。CERT 和 Microsoft 都发表了声明。媒体正在预言

Internet 的崩溃。IIS 管理员在一片慌乱之中安装补丁。但是，在这种混乱和恐慌之中，一些 IIS 管理员仍然能够保持(相对的)镇静。是什么使他们与众不同？很简单，他们花了时间来学习，并提前做了预防，在风暴袭来的时候已经准备好了。

在你读到这里的时候，Code Red 应该已经不是什么新闻了。但是，道理永远不会变。新的弱点会继续被发现，在它们被坏人利用之前，你需要理解它们并做好预防。本书中的知识能够使你成为在下一轮攻击中已经做好准备的人。好好地利用它吧。

——Todd Sabin

世界著名的安全程序员，不可或缺的 pwdump2 工具的开发者

前言

Windows 2000安全——是事实还是幻想

在1998~2000年间，Microsoft在服务器操作系统上所占的市场份额从38%上涨到40%，桌面系统从87%上涨到92%，Web浏览器从40%上涨到87%，以94%的比例获得了产品软件领域绝对的统治，甚至还使手持设备操作系统份额翻了一番，在即时消息领域也从0上升到38%(数据来源：IDC，Gartner)。

然而，很多媒体和安全权威机构都指责Microsoft的软件在安全角度上具有致命的缺点。如果Bill Gates的产品是那么的不安全，为什么它们还能这样流行呢？

Windows 2000安全缺口

答案十分简单。Microsoft的产品在设计上十分易于使用，这是它们得以迅速流行的原因。但很多人没有意识到，安全就像跷跷板：一个软件越易于使用，想要保护它就要花费越多的时间和精力。

这种平衡的一个很好的例子就是Microsoft的重要Web服务器产品——Internet信息服务器(Internet Information Server，IIS)。在Windows 2000中它是预安装的，而且已经完全配置好。任何人只要稍懂一些Web技术就可以在几分钟之内在IIS上建立并运行一个Web站点。

不幸的是，如果它被部署到Internet上，几天之内这个Web服务器就会被入侵者攻击并完全占领，他们拥有针对IIS的最新的攻击技术。

Microsoft也发布了一份题为“The Secure Internet Information Services 5 Checklist”的文档，列出了为保护IIS的安全而需要采取的一系列措施。这份文档没有随Windows 2000发布，它只能在Microsoft的Web站点上找到。在本书即将出版的时候，一种名为Code Red的“蠕虫”软件正在Internet上蔓延，侵袭没有实现这个清单中建议的IIS 5系统。有人估计，在蠕虫病毒发布后的14小时之内，超过345 000台服务器被感染。

我们之所以要编写此书，是因为Microsoft的原有配置和要使它的软件在真实世界中安

全运行所需的配置之间的鸿沟是如此之大。

用《黑客大曝光》填补鸿沟

我们将告诉你如何采用来自于最初的《黑客大曝光》一书的两种方法来填补这个鸿沟(现在它已经是第3版了)。

首先，我们将对你的Windows 2000部署会面临的最大威胁分类，并极为详细地解释它们是如何工作的。我们如何知道这些最大的威胁呢？因为世界上一些大公司雇佣我们进攻他们的基于Windows 2000的网络、服务器、产品和服务，为完成任务，我们每天都在使用它们。我们已经这样工作了3年多，研究最新公布的攻击方法，开发我们自己的工具和技术，并将它们综合成为我们认为是最有效地攻入现有的Windows 2000安全机制的方法。

在通过展示破坏性来吸引你的注意力之后，我们将告诉你如何防御每一种攻击。运行Windows 2000而不理解本书中的知识，这几乎就像开一辆没有安全带的汽车——在平整的路面上突然遇到了一个巨大的裂缝，而此时你的刹车已经坏了，油门也卡死在全速的位置上。

扩展《黑客大曝光》

除了与《黑客大曝光》所有相似点之外，本书在几个关键方面与它的主题有着明显的不同。显然，本书是集中于一种平台的，这与《黑客大曝光》系列的多平台不同。《黑客大曝光》考察了Windows安全领域，本书则进一步探索Windows 2000安全攻击和对策的细节，揭示那些让经验丰富的Windows系统管理员也会惊讶的内幕。正是这种深入彻底的分析使得它与《黑客大曝光》不同。探索很多其他计算平台的负担使得原书对一些主题的讨论停留在肤浅的层面。

本书对Windows 2000安全的讨论绝对不会浅尝辄止。它不仅囊括了《黑客大曝光》的所有关键信息和特点，它还在很多方面进行了扩展。在这里，你将找到克服Windows 2000安全缺陷所需的所有秘密知识——从系统的基本体系结构到未公开的注册表主键。

本书的组织

本书分为5个部分。

I. 基础知识

安全基础知识，以及从黑客的角度对Windows 2000安全体系结构的特点进行探索。

II. 侦察

在进行盗窃之前先到作案现场进行侦察。

III. 分而治之

从传统的正门入口——Windows文件共享服务(SMB)闯入，然后提升权限，扩大影响，抢劫，最后擦除痕迹。

IV. 攻击脆弱服务和客户端

通过常见功能攻击Windows 2000，包括IIS、SQL、终端服务、Internet Explorer和Outlook/Outlook Express、针对加密文件系统的物理攻击，以及拒绝服务攻击。

V. 防御

Windows 2000最新的安全功能、提示、技巧，对下一代Windows安全体系——代号Whistler和.NET Framework的预测。

章节安排：本书的组织方法

本书每个部分都由若干章组成，每章遵循一种明确的攻击计划。该计划是怀有恶意的黑客的方法，从《黑客大曝光》改编而来。

- 踩点
- 扫描
- 查点
- 渗透
- 提升
- 得到交互
- 掠夺

T

■ 扩展影响

▲ 清理

这个结构组成了本书的主干，如果没有具体方法，它们只是一堆没有内容和意义的文字。它是贯穿全书的进度图。

从第4部分开始，我们将进一步扩展这个结构，讨论渗透Windows 2000安全的其他几种方法(上面结构中的第4步)：

▼ 应用程序

■ 服务：IIS、SQL、TS

■ CIFS/SMB

■ Internet客户端

■ 物理攻击

▲ 拒绝服务攻击

第4部分将极为详细地讨论这些元素，演示如何利用它们迅速地攻入Windows 2000。

模块化、组织和可读性

显然，你可以把本书从头读到尾，获得对Windows 2000入侵过程的完整了解。但与《黑客大曝光》一样，我们试图使每章的每一节都尽量独立，因此全书可以分为很多模块，适合有目的的读者进行专项阅读。

此外，我们严格地坚持清晰、易读、简洁的写作风格，这在《黑客大曝光》第一版中得到了读者的极大反响。我们知道你很繁忙，你需要直接进入正题，不希望看到没用的废话。就像《黑客大曝光》一书的读者指出的："读起来像科幻小说，感觉像地狱一般可怕！"

你既可以从头至尾的阅读此书，也可以直接查找你所感兴趣的专题，本书的结构能够适应这两种阅读要求。

每章的"小结"、"参考和深入阅读"

为了改善本书的组织，我们在每章的最后都添加了两个新的题目——"小结"与"参考和深入阅读"。

顾名思义，“小结”将对本章介绍的主要概念进行简要总结，着重于提出安全对策。可以期望，如果你阅读了每章的小结，你将知道如何加固Windows 2000系统来抵御各种攻击。

“参考和深入阅读”含有寻找本章中的每个引用所需的超级链接、ISBN编号和其他信息，包括Microsoft安全公告、Service Pack(服务包)、热修复、Knowledge Base(微软知识库)文档、第三方的建议、商业化工具和免费软件新闻报道中的Windows 2000黑客事件，以及拓展本章中提供的信息的背景阅读。你在文章的正文中不会找到太多的链接——如果你需要它们，那么到每章的最后去寻找。我们希望外部链接的这种组织方式能够让你充分享受本书给你带来的乐趣。

附录：Windows 2000安全检查清单

在附录中，我们将本书中讨论的各种对策精炼之后，按照从头至尾的系统配置顺序将它们组织起来。是的，关于Windows 2000安全有很多的检查清单，但是我们认为这份清单是最实际、最有效的。

基本组成部分：攻击和对策

与《黑客大曝光》一样，本书的基本组成部分是每章中讨论的攻击和相应对策。

这里强调攻击，是因为它们贯穿了整个《黑客大曝光》系列：

这是攻击图标

我们以这种方式强调攻击，是为了易于识别专用的渗透测试工具和方法，给你足够的信息让你足以说服管理层为你新提出的安全措施投资。

与《黑客大曝光》一样，每种攻击都被确定一个危险指数：

流行度：	*用来攻击活动目标的使用频率，1表示极少使用，10表示广泛使用*
难易度：	*使用这种攻击所需要的技术难度，10表示很少或不需要技术，1表示需要经验丰富的安全程序员才能完成*

影响力： *攻击成功后潜在的损害，1表示只能获取目标的很少信息，10表示将获取超级用户账号或等价的后果*

风险率： *对上面的3个值取平均值并取整，得到总的危险指数*

在每种攻击(或一系列相关的攻击)之后，将给出防御对策。在讨论攻击对策的时候，本书与《黑客大曝光》有些不同。但对策图标是相同的。

这是对策图标

与《黑客大曝光》不同的是，我们在本书的每个对策中都添加了一个提要，给出如下数据：

厂商公告： *MS##-###*
Bugtraq ID： *####*
SP修正： *#*
日志签名： *是或否*

厂商公告一栏将以确定的格式，给出与提到的攻击相关的Microsoft官方安全公告。Microsoft安全公告中包括问题的技术信息、建议的解决方案或者软件补丁。可以使用公告编号在下述站点找到相应的公告：

```
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/
security/bulletin/MS##-###.asp
```

这个地址中的MS##-###就是实际的公告编号。例如，MS01-035表示2001年的第35号公告。

Bugtraq ID，或称BID，是Securityfocus.com的著名的Bugtraq邮件列表和弱点数据库对每种弱点赋予的跟踪编号。通过这个编号，你可以在下述网址查看Bugtraq清单：

```
http://www.securityfocus.com/bid/####
```

其中的####代表BID(例如1578)。我们选择使用BID而没有使用“通用弱点和揭露表示法”(CVE，http://cve.mitre.org)是因为Bugtraq的清单十分清晰，而且目前比较成熟。

“SP修正”一栏说明如果你已经安装了指定的Service Pack，那么这个问题就已经被修正了。

最后，“日志签名”表示这种攻击是否会在某种程度上被系统日志记录下来，于是该攻击能够被可靠地探测到，即使是在事情发生之后。

其他图形标记

我们使用了大量醒目的图形标记 **注意** 、**提示** 、**警告** 来强调经常会被忽略的一些极小的细节问题。

在线资源和工具

Windows 2000安全始终处在一种快速发展的状态中，我们知道印刷的文字不能有效地跟上这个充满活力的研究领域中出现的新东西。

于是，我们创建了一个WWW站点来跟踪与本书中讨论的主题有关的一些新的信息、修正，以及全书中提到的一些公开的工具、脚本和字典。这个网站的地址是：

```
http://www.hackingexposed.com/win2k
```

它还提供了一个论坛。你可以通过如下的电子邮件直接与作者联系：

```
joel@hackingexposed.com
stu@hackingexposed.com
```

希望你在阅读本书的同时，经常到这个网站上来查看更新的材料，获取我们提到的工具，或者是跟随Windows 2000安全的前进步伐。否则，就不知道有哪些新的发展会危害你的网络从而进行相应的防御。

给读者的忠告

撰写这本书我们花费了大量的时间，磨损了很多个鼠标垫，真诚地希望我们所做的全部研究和编写工作能够为负责保卫 Windows 2000 的你节省大量的时间。我们认为你部署Microsoft的操作系统产品是一个有胆有识的决策——但是在本书中你将会发现，当打开产品包装的时候，你的工作才刚刚开始。不要埋怨——继续阅读本书，在下一次Windows安全灾难到来之时，你将高枕无忧。