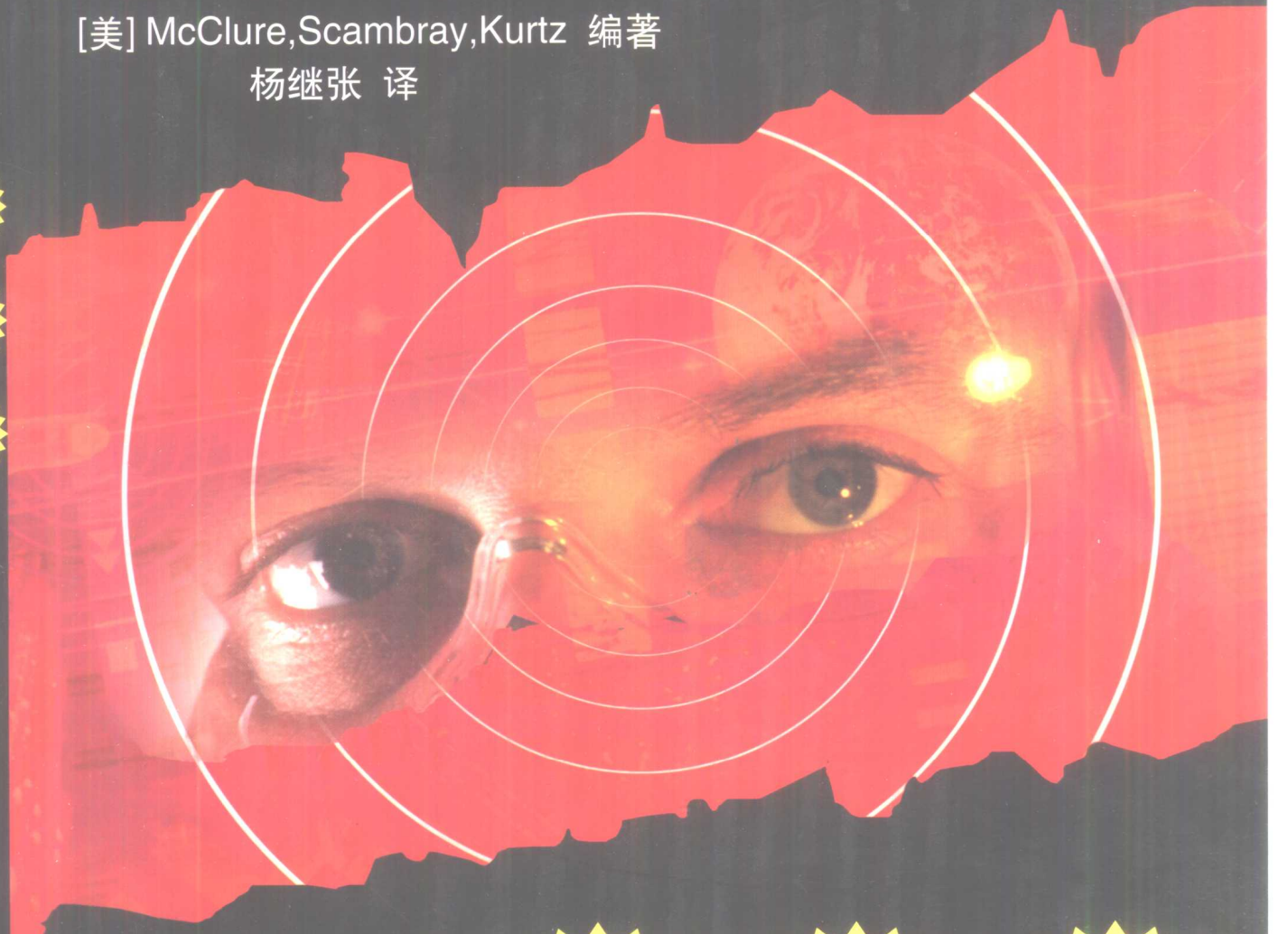
北京科海培训中心

[美] McClure,Scambray,Kurtz 编著
杨继张 译



黑客大曝光

网络安全机密与解决方案

清华大学出版社

McGraw—Hill 北京科海培训中心

黑客大曝光

网络安全机密与解决方案

McClure, Scambray, Kurtz 著

杨继张 译

清华大学出版社

(京)新登字 158 号

著作权合同登记号:01-2000-2241

内 容 提 要

本书从攻击者和防御者的不同角度,讲述了计算机和网络入侵手段与应对措施。

全书内容包括:从远程探测一个系统,标识其中的脆弱点到发掘特定操作系统(主要是 Windows NT、UNIX、Novell NetWare)上的漏洞的完整过程。轰炸拨打程序的应用、防火墙的规避、拒绝服务型攻击的发动、远程控制软件的滥用以及针对 Web 的攻击,也在本书的讨论之中。附录中还分析了 Windows 2000 的安全特性。

本书讲解了很多具体攻击过程,解释了攻击者确切想要什么,他们如何攻溃相关的安全屏障,成功之后怎么办等内容。本书特色在于几乎所有讨论过的攻击手段都有相应的对策。

本书适合没有太多时间研究安全保障工作的网络管理员和系统管理员阅读,也可作为对计算机和网络安全感兴趣的人员参考。

书　名:黑客大曝光

作　者:McClure, Scambray, Kurtz

译　者:杨继张

出版者:清华大学出版社(北京清华大学校内,邮编 100084)

印刷者:北京门头沟胶印厂

发　行:新华书店总店北京科技发行所

开　本:16　　印张:24.125　　字数:588 千字

版　次:2000 年 9 月第 1 版　　2001 年 2 月第 3 次印刷

印　数:8001～10000

书　号:ISBN 7-302-04000-1/TP・2346

定　价:43.00 元

本书献给 Melinda 和 Evan；要不是她们坚定的支持与理解，我的一生就几乎没什么值得一提。

——Stuart McClure

我把这本书献给我生命中的真正首要人物：我的妻子和女儿以及出生才一个月的二女儿。

——Joel Scambray

本书献给我亲爱的妻子 Anna。要不是她的理解、支持和不懈的鼓励，我不可能完成这本书。我还要感谢我的全体家庭成员，当最后期限看着就要逾越时，她们帮我“挤占时间”。

——George Kurtz

本书献给世界各地高尚的黑客们——但愿普通人们有一天会理解你们的信条：“知识与信息将让你获得自由。”

——全体作者

致　谢

首先，我们特别感谢全体作者的家庭成员，这一点是最为重要的。他们的理解与支持对于我们完成本书是关键性的。我们希望能够弥补上为完成这个出书计划而独自熬过的那段时间。

其次，我们每一位作者都值得另外几位作者拍下肩膀以示感激。光说这是集体努力的结果是有失偏颇的——我们依次感谢每一位作者，谢谢他为帮助完成本计划而支持另外几位作者度过了那么多个凌晨 3 点。

最后，本书得到了其他许多人的大力支持。我们感谢我们的同事 Martin Dolphin、ChrisProsise、Patrick Heim、Saumil Shah 和 Eric Schultze，谢谢你们对本书的许多方面提供了如此之多的帮助和指导。我们还感谢 Simple Nomad、Jeremy Rauchand 和 Mike Schiffman，谢谢你们在审阅本书若干章节上提供了大量的帮助和鉴定意见，并提供了极好的反馈意见。特别感谢 Jeremy Rauch 对 UNIX 一章的指导，并帮助编写了主要的代码。还得感谢 AlephOne 给我们提供了优秀的评注，帮助构思出一本更为完整的书。我们向本书中使用了的难以计数的工具的全体编写者们致以深深的鞠躬，其中包括 Mike Schiffman 和 Simple Nomad，不过需特别提及的是 Hobbit，他编写了我们最喜欢的工具之一——netcat，并就端口重定向提供了自己的指导意见。

我们还得特别感谢 Osborne/McGraw－Hill 出版社编辑出版本书的辛勤工作，他们是 Tara Davis、Jane Brownlow 和 Cynthia Douglas。最后感谢 Steve Turner、Andrew Lancashire 和其他所有尚未提及的人，谢谢他们在测试、调研和提炼本书素材上给予我们的帮助。

关于作者

Stuart McClure

Stuart McClure(CISSP, CNE, CCSE)是 Ernst & Young 公司电子安全解决方案业务部(eSecurity Solutions practice)的一位高级主管。McClure 先生是 *InfoWorld* 杂志安全观察(Security Watch)专栏的协作者,这是探讨时事性安全事务、漏洞发掘和脆弱性等内容的每周一期的全球性安全专栏。McClure 先生有 10 年以上在公司、学术机构及政府部门的网络与系统安全方面配置与管理的经验。他擅长攻击与渗透方法、安全评估审查、防火墙与连网安全体系架构、紧急情况响应、入侵检测以及 PKI 技术。McClure 先生加盟 Ernst & Young 公司之前的两年在 InfoWorld 测试中心工作,测试专门用于防火墙、安全审计、入侵检测和 PKI 产品的网络与安全软硬件。

读者可通过电子邮件地址 stuart@hackingexposed.com 与 Stuart McClure 联系。

Joel Scambray

Joel Scambray 是 Ernst & Young 公司电子安全解决方案业务部的一位主管,他在那儿向各式各样的机构提供信息系统安全咨询服务,特别是在攻击与渗透测试、主机安全评估、虚拟私用网络(VPN)连接、产品测试以及安全体系结构的设计、实现与审计上。Joel 参与编写 *InfoWorld* 杂志每周一期的安全观察专栏,发表了 10 多篇技术产品比较、评论和分析文章。他有 6 年以上基于操作性或策略性立场应用多种计算机和通信技术的工作经验,包括担任 InfoWorld 测试中心分析员的 2 年,以及在一家大的商业房地产公司担任 IT 主任的 2 年。

读者可通过电子邮件地址 joel@hackingexposed.com 与 Joel Scambray 联系。

George Kurtz

George Kurtz 是 Ernst & Young 公司电子安全解决方案业务部的一位高级主管,同时也是他们的剖析服务热线(Profiling service line)的全国攻击与渗透主任。Kurtz 先生在他的安全咨询职业生涯中完成了数百个防火墙、网络和与电子商业相关的安全评估。Kurtz 先生对于入侵检测、防火墙技术、紧急情况响应过程以及远程访问方案有相当丰富的经验。Kurtz 先生是颇受赞誉的课程"极端黑客攻击手段——防御你的网点(Extreme Hacking—Defending Your Site)"的领头教员之一。他是许多安全会议的固定发言人,并为多家出版物所引用,包括 *The Wall Street Journal*、*InfoWorld* 和美联社(the Associated Press)。Kurtz 先生给多家安全相关出版物写过若干篇文章。

读者可通过电子邮件地址 george@hackingexposed.com 与 George Kurtz 联系。

关于自愿投稿的作者

Eric Schultze

Eric Schultze 近 8 年来一直在涉及信息技术和安全，不过他的大部分时间花在 Microsoft 技术和平台上。他是安全方面会议的经常发言人，曾出现在多家出版物上，包括 *Time*、*ComputerWorld* 和 *InfoWorld* 。他目前是 Ernst & Young 公司 LLP 部门的安全专家之一，他在那儿给他们的 HackNT、AuditNT 和 SecureNT 服务热线开发了工具、培训课程和具体方法。Eric 以前的雇主有 Salomon Brothers 公司、Bealls 公司和 Price Waterhouse 公司。

关于技术性评阅者

Martin W. Dolphin

Martin Dolphin 是 Ernst & Young 公司在新英格兰的电子安全解决方案业务部的主管。Dolphin 先生有 10 年以上计算机管理经验，其中针对 Windows NT、Novell Netware 和因特网的安全方面经验有 5 年以上。他也给“极端黑客攻击手段——防御你的网点”课程上课。

Chris M. Prosise

Chris Prosise 专门提供安全方面咨询服务，在攻击与渗透测试、紧急情况响应和入侵检测上有丰富的经验。作为前美国空军军官，Chris 领导并完成了数十个安全渗透和紧急情况响应协约，给 *Fortune* 杂志评选的前 500 名客户开发了紧急情况响应方法，与人合作开发了 Ernst & Young 公司在 *Time* 和 *InfoWorld* 杂志上被作为特色的安全课程，并担任过教员。他拥有 Duke 大学电子工程专业学士学位，是经认证的信息系统安全专家(CISSP)。

前 言

Marcus J. Ranum (mjr@nfr.net)

黑客攻击是一种既令人兴奋、有时又让人害怕的现象，这取决于你碰巧站在哪一边的立场上。在构织成现今电子市场之骨干的由彼此联结的系统和软件组成的大网中，似乎每天都有人发现一些新的脆弱之处。在墙的一侧即里边是疲惫不堪的网络主管和安全专家们，维护和构筑现代生活中日益重要的计算机网络是他们的责任。在墙的另一侧则是一群光怪陆离的黑客，他们以指出墙上的每个裂隙为乐，办法是定期公布特别是那些趾高气扬的防御系统上的漏洞。

还有一些罕见的个人——私人情报侦探——跨骑在墙上，他们了解并公布关于敌人所用伎俩的信息。本书的几位作者就是这样的个人。

至于我们其他人，没有一个感到百分之百的安全，然而为避免成为可能的攻击目标而坚持不懈地维护防御体系所需的时间和精力，也没有几个人花得起。计算机安全是个令人感兴趣的使命：挑战与挫折并存，偶尔又让人极端兴奋，总之就是大量的工作。不幸的是，构筑计算机网络本身使得所剩时间无几，难以再尽这些侍卫们的职责。

对于那些确实负责保障关键系统的安全，每天又深感时间和资源之紧张的人来说，他们的武器库需配备一件必不可少的武器：信息。如果你正在读这句话，那你所捧的书里包容的就是一些非常有用的信息，因此别放下！市场上有许多安全方面的产品，销售各种解决方案的厂家也不少——然而要是你不理解那些产品和厂家实际在干什么以及它们是如何帮助你的，那它们也无法真正帮助你。躲避夸夸其谈的解决方案及问题的唯一最佳办法是了解哪些能起作用，哪些不起作用，以及为什么。这就是本书的立意。我跟许多这样的用户共事过：他们将敏感的信息——商业记录、与所爱的人之间来往的电子邮件、在线付款软件、交税情况等——在线放置在自己的 PC 机上，而这些 PC 机又被冒冒失失地连接到了因特网上。他们应该感到害怕，但是他们并非如此。正在发生中的黑客攻击活动的具体数量难以估计，不过我可以给你提供几个参考数据。我的机器每星期被人探测数十次。我的一位使用电缆调制解调器的朋友每天被人探测数十次。探测这些机器的黑客们所用的就是几位作者在本书中讨论的那些把戏；本书提供了破解这些把戏的对策。

本书的几位作者具备丰富的网络安全的防御经验。为了获取这方面的经验，他们对攻击者们所用的方法做了大量的研究，包括他们的工具、他们的技巧以及他们在什么地方交换攻击秘密。本书到处都是这类内容。到阅读完本书时，你们中某些人可能会感到比在开始阅读之前更为焦虑不安。本书的未尽之言是："是的，你确实如此之脆弱。"要是这几位作者仍没有说服你需要采取措施以加强系统的安全，那就没有办法能够说服你了。

黑客们都知道这些技巧，而且会毫不犹豫地把它们用在你头上。为此几位作者给你提供了对策和许多有用的建议。黑客们采用的大多数攻击手段是使用简单的工具扫描整个网络，以期发现"低垂的水果"——防御薄弱的易攻目标。对这些基本的薄弱环节加些支撑就能让

你摆脱作为具有代表性的典型防御水平的厄运，坏小子们会因你这颗坚果太硬不易敲开而绕道。不要因为自己是一个不起眼的或不令人感兴趣的目标而自欺欺人地认为自己安全——黑客们使用的自动扫描工具并不进行这样的区分。请严肃地对待本书中的建议；它们是合理的好建议。

许多安全专家因本书揭示了某些技巧而感到不安。他们的逻辑是："如果我们讨论这些技巧，那是在鼓励黑客们尝试它们。"这也许是对的，然而现今的黑客们所用的交流和信息共享方式比安全专家们所用的还要好。为了获取解决某个问题所必需的资源，网络主管们有时候不得不非常遗憾地演示确实存在该问题；也许本书单独就能起到这样的演示作用。我在加强系统安全性上得出的经验是，大多数用户一旦发现自己实际上有多脆弱，他们就会震惊不已。也许本书会让你震惊。不管怎么样，它肯定会让你得到教益。

Marcus J. Ranum
1999 年 7 月 28 日

Marcus Ranum 自 1988 年以来一直在设计并部署因特网安全系统，当年他构造了第一个商业防火墙产品 DEC SEAL。在来自 DARPA 的一笔研究金的资助下，他于 1992 年编写了 TIS 防火墙工具包，用于开发保护美国总统的电子邮件系统(whitehouse. gov)的防火墙技术。Ranum 先生目前是 Network Flight Recorder 公司的首席执行官，这是一家制作业界最为流行且效率最高的入侵检测系统的公司。他是国内和国际会议上频频露面且颇受尊敬的教员和发言人，担任着若干家高科技新兴企业的董事会职务，并作为一位安全产业分析员给国内的杂志和投资银行家提供咨询。他家在马里兰州，跟一小群猫住在一起。

简　介

0.1　本书写作动机

我们这下子引起了你的注意，因为你正在阅读的是一本关于入侵计算机网络的书。

是什么样的动机促成一个人去写一本暴露如此地具有颠覆性和潜在危害性的话题的书的?这是一个敏感的问题，同时也是大家应对书架上围绕本书放置的其他许多计算机安全书籍提出的问题。有关揭露恶意的黑客及他们所用手段的书已不鲜见，不过其中不少是随着近来大众媒体上涌现的大肆渲染之势而仓促写成的，它们对为此发热的人们推波助澜一番后马上就销声匿迹了。我们这本书可不是这样。

我们确实想以平实的易于理解的说法给人们提供详尽的攻击计算机网络的具体步骤。

不清楚信息系统安全之历史的任何人都可能震惊于我们刚才说的这句话。甚至于专职从事计算机安全工作的人们(譬如说我们)偶尔也会质疑这句话是否明智。然而不管你信还是不信，自从许多年前不大昂贵的多用户计算机系统面世以来，没人提出过更好的保障网络之安全的思想。回溯当时，专门针对公司计算机设施执行渗透测试的所谓"虎仔队(tiger team)"组建了起来，他们是有人付钱的在思想倾向上充当坏人的好伙计。在作为底层支撑的计算机平台本身经历了许多重大沿革之后，这种思想仍与我们保持一致。

多年来计算机技术在迅速地发展，然而为什么至今还没有人发明出"完美的安全机制"呢？是什么原因导致这种间谍式的做法成为必要的呢？这是大多数人最为困惑不解的问题之一。这个问题的答案存在多个因素，从现代软件开发中内在的的错误到网络连接的无所不在都包括在内，不过基本上可归结为大多数人都能理解的一句话：世界上没有完美的设计。

因此，任何攻击者不论是否好意，所运用的最有效的武器就是找出一个系统中存在的瑕疵的能力，而这些瑕疵对于其设计人员和日常使用人员来说并非一目了然。正如一位著名的安全专家说过的那样，改善自己的网点的安全性的最佳办法就是尝试入侵它。①

本书的目的就是公开讨论攻击者们常用的技巧和工具，借以展示他们所发掘的漏洞，从而有可能永久地关闭它们。当然，如此坦率的讨论是利害参半的：我们在这儿详细探讨的技巧和工具很可能被攻击者用于恶意的目的。我们并不宽容这种行为，但是有所了解并因而有所防范总比成为单纯的受害者要好。本书涵盖的所有内容在因特网上都能找到，它们分散在数千个网页、匿名 FTP 网站、因特网 IRC(中转交谈)服务器、Usenet 新闻组以及数不清的其他资源中。我们所做的就是把这些知识编纂归结起来，并以自己的经验简化、组织和充实它们，从而使得它们变得唾手可得、易于消化且方便速查。

毕竟，你又何必做个网络上唯一未经武装的成员呢？

---

① 译者注：网点一词的含义参见译者译著《UNIX 网络编程(第 1 卷)》第 166 页译者注 1。]

0.2 本书的读者群

要是你还没有留意到的话，可以明确地告诉你我们确实喜欢安全，而且我们是如此之津津乐道，以至于觉得很有必要告诉别人。不过不是任何人都行。本书是为我们的网络管理员同事们写的，他们工作负荷重，收入又偏低，几乎没有足够的精力让事情运作在一个能被接受的水准，更不用说安全水准了。遍查因特网上最为黑暗的区域，把自己连续几天禁闭在模糊的技术手册中，义无返顾地努力理解拥有、运行或使用计算机网络的任何人被迫直接面对的威胁的性质和程度——这些我们在做的事情并不是所有网络管理员们都可能有时间或兴趣去做的，对于他们来说，我们期望本书可用作安全的入门书。

就像以网络管理员为读者对象的其他书籍一样，我们要求你具备计算机网络技术的中等熟悉程度，特别是对因特网。不过如果你的理解面比较高层而欠缺技术性，那也不必担心。我们会一步一步地引导你掌握具体细节，并以对于终极用户和主管们来说都合理的方式解释攻击技巧的主要特点。技术性较强的读者毫无疑问也会从中学到不少东西，因为我们常常发现即使是有经验的管理员也未曾仔细地考虑过如何攻击自己花了那么多时间架构起来并加以支持的技术。到看完本书时，你甚至会同意这样的观点：了解自己的计算机网络的安全现状的最佳办法是尝试入侵它。

有许多人指责我们写了一本对于网络管理员的身心弊大于利的曝光性书；要是他们稍微仔细地阅读过本书，那就不会这么认为了。书中伴随每个脆弱点和漏洞发掘过程的讨论的是建议的对策，这样当你发现自己的网点存在某个脆弱点时，就可以修复它或监视试图发掘它的攻击者。在思想开明人士看来，本书将帮助你尽快掌握谁有可能以何种手段在什么时间从什么地方针对哪个或哪些漏洞入侵自己的网络，这么一来，当有人很想知道“我们究竟有多安全?”时，你就可以睿智而权威地给出回答。

关于“黑客”和“垮客”的说法

网上社区已就“黑客(hacker)”一词的用法对主流媒体高谈阔论了若干年，即“黑客”是入侵计算机系统的个人的包罗性定义。按照传统说法，“黑客”指称为了领悟大家不熟悉的系统的机理并且/或者把它们改造得更好而以无私的努力精心琢磨它们的英雄。① 相反，“垮客(cracker)”一词指称为了好玩或盈利目的而入侵系统的邪恶黑客。②

语言以其自身的方式演变，“垮客”一词从未发展成指代计算机犯罪者们的主流口语词汇。尽管我们觉得“垮客”这种说法也不完全合适，但是几位作者仍对“黑客”不必是坏人的观念深表同情(事实上我们自认为是合乎道德的黑客)，并在本书中避免使用“黑客”一词来归类在自己的系统上研究和试验计算机安全的人们。@[译者注：尽管如此，hacking 一词也只好译成黑客攻击。]

① 译者注：一般以大写的“Hacker”或“HACKER”尊称这种意义上的黑客，伟大的 GNU 项目(Web 网站地址为 www.gnu.org)的发起人 Richard Stallman 先生早在启动该项目前就已经是闻名遐迩的这种黑客了。

② 译者注：cracker 一词台湾人译成怪客。这种译法虽切音但不切义，译成垮客既切音又切义。

另一方面需要强调，对于未经授权擅自访问他人资源的任何人，我们跟有良知的人们一样毫不同情。不论“黑客”一词的定义具体怎么样，这是我们划定的区分正义与非正义的界线。因此，为了给窃取计算资源访问权的不良企图归类，我们尽可能使用更为明确的称谓，例如“邪恶的黑客”、“攻击者”或“入侵者”等，另外，要是我们无可避免地出了漏子，搞混了这两个极端间的区别，那么我们乞求读者们的谅解（是的，我们肯定存在这样的漏子）。

0.3 本书的组织

尽管我们对本书每一个词都感到满意，并期望你会阅读完整本书，我们还是现实地预期到许多读者没有足够的时间。你可能很忙——这也许是你一开始捧读本书的原因，即汲取修复漏洞的关键点和具体建议，然后抛到一边。因此从本书中获取最大信息量的方法有两种：一是各取所需，二是从头到尾。

0.3.1 各取所需方法

我们已把本书的结构按模块加以划分，因此可作为一本参考手册看待。每章彼此独立地设计，涵盖某个特定的技术和平台，这样你就可以选择与自己的环境最为贴切的那几章来阅读，而不必涉足不相干的信息。每一章内我们又按照定义完备的攻击方法与对策，努力把内容组织成便于消化的一个个篇章。这么一来，你就可以把火力集中到对自己最为重要的问题上。

0.3.2 从头到尾方法

对于时间充裕兴趣浓厚的读者来说，本书从头到尾贯穿着一个综合的话题。这个话题就是入侵者的基本攻击方法学：

- 目标探测与信息汇集
- 初始访问
- 特权升级
- 踪迹掩盖
- 后门安置

成功的计算机入侵活动一般都在事先仔细计划，并按照本方法学一步一步地进展。正如我们所说，这条路途上每一步都可单独访问，不过要真正欣赏网络入侵之“道”的话，还得从头到尾地阅读本书。

0.3.3 对策

最重要的是，我们花大力气反击本书中讨论到的每种攻击手段，提供相关的防御技巧。我们给这部分内容冠以“对策”的标题，它们通常就紧跟在对每种攻击手段的讨论之后。某些情况下我们先连着讨论一组关联的入侵技巧，再给出对付这些攻击手段的综合对策。我们希望本书中列举的某些攻击手段的简易性足以让你感到害怕；同时，我们也不会让你在阅读完

之后仍然束手无策。

终极对策:选好保密字

我们希望本书提供的大量技术细节和花样繁多的题材并没有导致读者忽视处处提及的最为平庸却又是压倒一切之重要的对策:强壮的保密字。尽管计算机在其他大多数领域已取得长足的进步,安全领域却仍然由保密字这只信天翁肩负着。要是你从本书中就如何改进自身网络的安全得出某个想法的话,那它应该是彻底地实施保密字复杂度保证策略;它可能解决本书讨论到的问题中的90%。

0.3.4 个案研究

作为本书四个主要部分的引子,我们分别提供一个来自现实世界计算机安全事件的个案研究。选择这些装饰性短文的目的是一定程度地让你感受黑客们的思想(不论是否恶意),并给出后续技术信息的上下文。

0.3.5 各个部分

本书划分成以下几个部分:

第1部分:窥探设施

任何有头脑的入侵者在尝试获取访问目标系统的特权之前,都要预先进行工作量可能不少的调查研究。这一部分具体分析恶意的黑客可能用来刺探潜在目标的某些技巧,介绍如何识别这些活动,并提供拒绝给予攻击者们梦寐以求之信息的方法。

第2部分:攻击系统

这一部分介绍黑客们一旦侦察完地形就可能施行的攻击。内容涵盖包括Windows、NetWare和UNIX在内的主流操作系统平台中发现的漏洞;攻击者征用这些系统发动进一步攻击或者随心所欲地耗用它们的CPU周期的手段,以及至为重要的用于掩盖踪迹的方法;攻击者们遗留的暗示有不速之客光顾的蛛丝马迹也在讨论之列。从保密字破解到操作系统本身固有的瑕疵——你读完本部分每一章之后,就会明白入侵者们是如何空穴来风地侵袭的,同时了解如何锁固自己的系统,将系统的被侵袭概率有效地降为零。

第3部分:攻击网络

计算机并不是存在于网络上的唯一实体。这一部分详细介绍攻击者们如何利用诸如拨号服务器、路由器、防火墙等设备甚至网络协议自身存在的低层缺陷来窃取他人的宝贵数据。你读完本部分每一章之后,就能知道如何在自己的网络周边设置严密的封条。

第4部分:攻击软件

这一部分从基础设施的问题往高层再进一步,探讨成了各地安全专家之祸根的应用程序本身的问题,包括远程控制程序、后门陷阱及Web服务器软件。了解如何标识并清除由这些软件实体构成的威胁是对自己的计算机和网络环境作封舱处理的最后一步。

第5部分:附录

这一部分是计算机安全方面资源的珍藏处,布置条理并有说明,方便读者速查。内容包

括在线资源和超链接的汇编、关于 Windows 2000 的安全问题与解决办法的讨论、自由软件或商业软件性质的安全工具清单、典型攻击方法学的流程图以及像 TCP/UDP 端口明细表这样的有用信息。

所伴 Web 网站上的内容

伴随本书的 Web 网站地址为 http://www.osborne.com/hacking，我们的个人网站 http://www.hackingexposed.com 也提供同样的内容。该所伴网站提供大量的第三方工具以及我们从多年的渗透研究中累积下来的自己编写的脚本。这些工具的意图是辅助工作繁重的网络管理员。我们假定不会有人拿它们来干坏事。

关于在线资源的一个注意点

本书无处不在地淹没着对于原始研究材料、二进制可执行文件及程序源代码的参考点，它们都可以从因特网上获取。因特网上每天都在极为详细地讨论着计算机安全的现状，因此不上网查看是不可能完整地钻研这个主题的。

关于测试环境的建议

我们已花大量时间测试过本书中涵盖的每个漏洞的发掘过程，因此你不必再这么做。不过为了充分赏析里面的各种技巧，你确实应该亲自尝试。为此，我们建议你架构一个或许只有两三台廉价的 PC 机的小型测试网络。其中至少有一台计算机必须运行某个 UNIX 变种操作系统。运行 Windows NT Server 和/或 Novell NetWare 操作系统的计算机也得有，具体取决于你自己的“实际”网络的构成。我们的内部测试环境的标准拓扑是以太网，不过你的测试环境可能需要调整，以反映自己的实际环境。TCP/IP 则是必需的。

0.4 以后的做法

确保有一台能上因特网的计算机在身边，并着手翻动网页。最好随身带个笔记本，这样当你从本书中看到自己的网络不可避免地也存在可能会被别人发掘的漏洞时，就可以草草地把它们作为待检查的提醒事项记录下来。像我们早先建议过的那样，着手考虑你自己的测试网络的搭建事体。黑客攻击是一种接力运动，你应该开始摆开双臂尽可能快地紧步赶上。

我们最后重申解放思想的重要性。按照定义，黑客攻击就是凭某人的创造力和智慧发现别人看来是不可穿透的铜墙铁壁上的漏洞。只有处于黑客们的心智开放状态下，你才有可能正确地评估自己的网络的安全性。我们会努力帮助你形成这种思想倾向，不过归根结蒂，你是否愿意认识和了解自己的基础设施中存在的瑕疵将决定你能否成功地保障它的安全。

目 录

第1部分 窥探设施

第2部分 攻击系统