系统与安全丛书

PEARSON Prentice Hall

拦截黑客

——计算机安全入门（第2版）

HALTING THE HACKER

a practical guide to computer security
second edition

[美] Donald L. Pipkin 著

朱崇高 译

网络安全顶级专家教你如何对付黑客

hp invent

清华大学出版社

系统与安全丛书

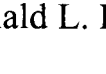
拦 截 黑 客

——计算机安全入门

（第 2 版）

[美] Donald L. Pipkin 著

朱崇高 译



清华大学出版社

北 京

内 容 简 介

本书从黑客的角度对信息系统进行了观察。通过诸多信息系统受损的突出事例对黑客如何访问信息进行了描述，同时也就如何避免类似损失展开论述。

无论读者是一名初学者还是有经验的安全专家，本书都是一种不可多得的资源，不仅为技术人员也为非技术人员提供了有用的信息。适用于网络安全技术人员和网络系统管理员阅读。

EISBN: 0-13-046416-3

北京市版权局著作权合同登记号　图字：01-2002-6531

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目（CIP）数据

拦截黑客　计算机安全入门（第 2 版）/[美]皮普金著；朱崇高译. —2 版.—北京：清华大学出版社，2003

（系统与安全丛书）

书名原文：Halting the Hacker：a practical guide to computer security, second edition

ISBN 7-302-06798-8

Ⅰ.拦…　Ⅱ.①皮…　②朱…　Ⅲ.计算机网络—安全技术　Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2003）第 054509 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）6277 0175　　**客户服务**：（010）6277 6969

文稿编辑：葛昊晗

封面设计：立日新设计公司

印 刷 者：北京牛山世兴印刷厂

发 行 者：新华书店总店北京发行所

开　　本：185×230　　**印　张**：20.75　　**字　数**：504 千字

版　　次：2003 年 8 月第 1 版　2003 年 8 月第 1 次印刷

书　　号：ISBN 7-302-06798-8/TP・5059

印　　数：1～3500

定　　价：39.00 元

序

数年前，很少有人关注计算机安全问题。那时，这一话题仅与学院、金融机构和政府保密部门密切相关。如今，在世界范围内，普通大众对计算机安全已不再陌生，人们尤其对计算机病毒、网上个人信息隐私以及 Internet 交易信用问题了如指掌。

由于全球经济对计算机和 Internet 的依赖与日俱增，因此这些设备的安全性、可靠性和隐私问题显得极其重要。网络攻击，无论它来自未成年黑客还是死心塌地的恐怖分子，都会导致敏感信息的泄露、严重的系统破坏和 Internet 秩序的混乱。因此，从商业和技术角度出发，人们应该了解如何尽量降低风险，以及如何保护关键性的基础设施、系统、应用程序和数据，这一点比以往任何时期都更为重要。

组织必须执行一项评估，以了解自身面临的威胁、出现这种威胁的可能性以及被人利用后的危害程度等。风险很少能够消除，但必须设法将其控制在可以接受的水平上。接入 Internet 后个人和企业都会从中得到很大好处，但这也会给他们带来大量的风险。有些威胁由于不太明显而被人们忽视。然而，由于人们错误地认为自己不会受到影响，他们往往会忽视一些显而易见、后果严重的威胁。

Don Pipkin 在计算机安全领域有着多年的实际经验，这些经验使他能以“黑客的眼睛”来探究计算的环境。这种视角有助于读者了解他们所面临的来自黑客的威胁以及成为黑客“理想目标”的原因所在。黑客的各种行为实例贯穿《拦截黑客》的所有章节，这些实例既能激发大家的阅读兴趣，同时也证明了这些威胁并非仅仅是一种假设。虽然这种内容具有很强的娱乐性和知识性，但最为重要的是作者就如何消除这种威胁进行了论述。将这种知识付诸实践能大大降低成为攻击目标的可能性。此外，本书还提供了一些有益的指导，以便在黑客对系统进行攻击时有所准备。

本书第二版对原有内容进行了扩充，收录了最近几年内出现的许多漏洞利用方法。无论读者是一名初学者还是有经验的安全专家，对他来说，本书都是一种不可多得的资源。同样，《拦截黑客》不仅为技术人员也为非技术人员提供了有用的信息。

2001 年 9 月 11 日发生的灾难性事件大大增强了公众的安全意识。社会对技术的依赖

使人们意识到，必须改进计算基础设施，减少迄今为止被人们忽视的许多风险，否则，就会导致严重的业务混乱，而肇事者甚至无需进入受害国的领土。比以往任何时候更为重要的是，应该进行适当勤奋的努力，以确保全球计算基础设施的安全性。遵照《拦截黑客》中提出的指导性建议采取行动是实现这一目标的重要一步。

Craig Rubin
信息安全设计师
Internet 安全解决方案实验室
惠普公司

前　言

在计算机的发展历程中，黑客从未有过如此美妙的机遇。计算机的价格不断跌落，而性能则不断攀升，这使得任何黑客都能拥有一台属于自己的功能强大的计算机系统。低价、高速的 Internet 接入几乎遍及每一个角落。黑客工具随处可得、使用方便，这使得任何人都能够成为一名黑客。

与此同时，企业使用信息系统的方式也在发生不同寻常的变化。公司的规模日益缩小，从专用大型计算机衍变为开放式系统，办公室个人计算机中的信息迫切需要在全球范围内共享，企业纷纷涌向 Internet，以便为客户提供新的交易渠道，于是，远程移动办公族或在家办公族应运而生，专用私人网络也被廉价的虚拟私有网络所取代。随着计算机数量的增加和网络连接的扩展，国际网络系统已能为计算机提供空前方便的接入服务。

财务压力迫使一些公司开始寻求新的机会。业务外包成为许多公司的选择，它们与合伙者达成新的业务组织方式，这种方式要求公司与远程的非正式人员共享更多的信息。对许多急于联网的公司来说，这些新的环境尚属未知领域。公司、管理人员以及用户都必须改变自己对计算环境的理解，应该用新的规则来使用、管理和评价这种新的环境。公司通过裁员来控制成本，这就导致许多新系统的诞生，这些系统的使用者都是些缺乏经验的管理者，他们负责应付大量的计算机系统，并对它们的操作系统知之甚少。系统易于访问，管理者工作繁重、缺乏经验，这些因素结合在一起将构成一种潜在的破坏性。

许多公司采用基于 UNIX 系统的操作系统——原因之一是大型机的尺寸日益缩小，原因之二是 Linux 是一种免费操作系统，最后一种原因是他们对选择感到厌倦。操作系统越普及，就越容易引来黑客的袭击。UNIX 系统一般为大学和研究机构所采用。由于它广泛应用于科研领域，因而有关这一系统的信息非常丰富。此外，大学和科研机构在安全性方面通常比较松懈，这就为黑客了解和攻击系统提供了用武之地。UNIX 操作系统是文档最为齐全的操作系统，各种版本的源代码随处可得，这使得它成为当今黑客经常攻击的目标。

在计算机行业中，在大多数情况下，往往是在出现问题后才考虑安全性。人们通常认为添加不必要的安全措施只会给程序带来麻烦。大多数软件系统都是由以往的系统演变而来，而且事实上一些大型软件系统往往包括来自诸多方面、由多位作者编写的代码。如果你使用的不是一种单独设计的软件，那么出现问题后再嵌入安全功能几乎是不可能的。

本书根据黑客进入系统、获取特权以及控制计算机系统时采取的步骤来组织内容，而不是简单地论述应该如何保证每一个软件子系统的安全性。这有助于您了解如何协调使用不同的子系统来攻击计算机，以及改变某个系统将如何影响另一个系统，并最终使计算机系统彻底失去安全性。本书阐述了某个问题被操纵和转化为安全破绽的原因和途径，并就如何修补这种破绽进行了探讨。理解问题的“原因所在”将是大家在整个职业生涯中享用不尽的一项技能。

本书第二版详细论述了构建和保护 UNIX 系统的过程，并专门就 HP-UX®和 Red Hat® Linux®系统进行了深入探讨。

本书对黑客进行了细致入微的审视，揭示出一些普遍性的动机和常用的基本方法。这样做是为了使系统管理员了解如何有效应用安全措施长期确保系统的安全性。

关于作者

信息系统安全认证专家（CISSP，Certified Information Systems Security Professional）Donald L. Pipkin，是惠普公司 Internet 安全部门的一名信息安全设计师。他已在这一行业积累了十五年多的工作经验，是一名享有国际声誉的安全专家。他经常就安全问题发表演讲，并推出新作《信息安全：保护全球企业》。他精通安全工作的方方面面，包括策略和规程等，并掌握了有关计算机入侵的一些实际经验。他还在各种地方性和国际性会议上就安全问题发表演讲。凭借多年的经验，他挥洒自如地运用自己对安全问题的理解和有关应对计算机犯罪的经历就解决特定安全问题的策略和规程问题向《财富》杂志前 500 名公司提供咨询。

致　谢

在此我要感谢所有对本书第一版提供反馈信息的读者以及在课堂上采用本书的教师们。尤其要感谢那些在本书创作过程中协助过我的人们，特别是 Chris Cooper、Gary LaBeau、Ken Privette 和 Craig Rubin，他们的评论为进一步提高本书的质量提供了宝贵的建议。

最后，还要感谢我的妻子和孩子们，他们牺牲了和我共处的时间，使我得以完成此书。

Donald L. Pipkin, CISSP

目　　录

第Ⅰ部分　了 解 黑 客

第Ⅱ部分　黑客活动过程

第Ⅰ部分　了解黑客

重要的是了解你的对手。了解对手能够使您预料黑客的行为和动机，以便能有效地避开攻击。破坏信息系统的人涉及面很广，他们动机各异，技术水平也参差不齐。要了解可能对你的系统进行攻击的黑客，就应该明白自己为什么会成为攻击目标。系统之所以成为攻击目标，可能是因为它们包含某种信息，或者因为通过它们可以访问一些特殊的资源，也可能因为系统过于脆弱。系统遭受攻击的原因可能涉及财务、政治、个人等方面，或者仅仅因为它们有利的地点或易于访问。攻击方式可以是简单的脚本袭击，也可能是处心积虑和有组织的进攻。也有闪电式的袭击或现场攻击。攻击和攻击者的极度多样性增加了对系统管理员的要求，并要求他们对黑客环境有一个总体的认识。

黑客活动的环境

真正的黑客必须有一台计算机、网络连接和进行黑客活动的时间。黑客一般使用的是Linux 计算机和高速网络连接，他们通常是一些学生或在工作中享有充分自由时间的从业者。这正好符合大学环境，因此大学已成为黑客聚集的场所。学生们可以使用一些功能强大并与高速网络连接的计算机，而且他们还有充足的时间。然而，所有这些特点正日益在家庭内得到普及，如今，家庭计算机已达到很高的速度，价格也非常便宜。始终在线的高速网络也通过 DSL 和电缆网络进入了普通家庭。

Linux 是黑客普遍选用的操作系统，因为它能运行绝大多数工具，而且具有很强的灵活性，能控制系统的任何方面。一旦拥有属于自己的计算机，黑客便能成为受攻击系统的对等用户，而不仅仅是一名访客。利用自己的系统，他还可以对权限和特权进行控制，这样，他就能在外部系统以自己所希望的身份出现在被攻击系统。他还能因此而获得管理和保护计算机的经验，从而深入了解自己的对手——系统管理员。为了避免遭受外来攻击，他需要对自己的系统进行管理和保护，以便知道是否有人在探测自己的系统。一旦察觉到黑客，系统管理员就会努力识别系统攻击者。

黑客拥有的网络带宽越大，他进行扫描、探测和攻击的机会也就越多。带宽往往是访问远程系统的限制因素。

历史透视

黑客是伴随着计算机系统的诞生而出现的。早期黑客都是一些学生，他们总是试图访问超出分配范围的计算机资源。因此，他们希望找到获得这些非授权资源的途径。他们也许会“找到”用来运行程序或存储文件的其他账户，也可能会黑掉（篡改）账户设置软件，以便免费使用这些资源。当时，所有人——包括教师——都对计算机抱有一种新奇感，因此人们更为关注的是这些黑客所表现出来的创造能力和聪明才智，而不是盗用资源所犯下的罪行。然而，这些黑客活动仍然属于盗窃行为，即使它们可能只被视为一些小小的罪行。

长期以来，随着计算机的普及，计算机犯罪的数量和类型越来越多，其严重程度也不断攀升。如今，被确定为黑客的计算机罪犯，其多样性令人倍感震惊。当黑客活动初露端倪之时，黑客大都是一些能对系统进行访问的学生。目前，这类黑客仍然是一个庞大的群体，不过一些动机不良的专业人员也加入了这一行列。

现在，“黑客行为”一词的含义通常是，未经许可秘密侵入计算机系统，以及通过或针对计算机进行的犯罪行为。计算机犯罪可以追溯到20世纪70年代早期，当时，为了侵吞雇主资产，一些员工设法利用计算机来篡改销售记录。这些黑客所造成的损失高达数百万美元。

本书并未根据黑客意图来划分其内容。黑客的真实意图并不是本书探讨的问题。任何未经许可对信息系统进行访问的人都是在犯罪，都有可能造成损害。他们会给系统所有者带来时间和金钱上的损失，因为他们要对事件进行调查，以确定黑客做了些什么以及是否造成了损害。至于所造成的损害，无论是有意的还是无意的，都必须进行修复，同时也要对这种损害给业务带来的影响进行评估。此外，还必须确定侵入方法，并对系统进行相应的修正，以排除事故复发的可能性。

黑客或骇客

目前，黑客这一术语还存在着争议。一些人反对用它来描述计算机罪犯，他们指出，它最初用于形容那些能迅速编出所需代码的人们。这类代码编写仓促，不考虑设计效益和可维护性。黑客对系统的理解能力似乎来自他们的直觉。黑客行为意味着为了挑战自己的智慧而对计算机系统进行无拘无束的探索。黑客一词变得更加神秘莫测：一位电脑奇才，他能使系统完成任何自己所希望的工作。不过该词的普遍用法仍然侧重于表示那些已经开始对ARPA计算机网（Advanced Research Projects Agency Network，美国国防部高级研究计划局建立的计算机网）——Internet的前身——展开探索的人们。这些黑客经常在未经许可的情况下对远处的系统和系统信息进行访问。另一些人则将黑客视为偶像，认为他们是

一群热爱计算机的精英分子，这些人对黑客一词的普遍用法感到不快，于是，他们想出了“骇客”（破坏者，cracker）一词，用来表示那些闯入系统或在进行黑客活动时有任何犯罪行为的人。

在谈到这一话题时，《2600》杂志的编辑 Emmanuel Goldstein 说：“目前，我们发现，有一小撮畅所欲言的人，坚持将那些他们认为在黑客世界里所有无法接受的人称为‘骇客’。他们试图通过简单地误用一个新词来解决对黑客一词的误用问题，这是一种善意但极其错误的作法。”[①]

然而，人们所知道的有关早期黑客活动的许多情况都是通过黑客团体流传下来的故事，这些故事倾向于美化黑客，诋毁任何试图阻止他们的组织。上述一小撮畅所欲言、试图“保护”黑客一词的人们并未得到多少支持。大众媒体继续使用黑客一词来表示计算机罪犯，这也是这些罪犯对自己的称呼。

自我定义

也许，在有关黑客一词用法的争论中，最为重要的说法来自那些未经许可对系统和信息进行访问的人们。他们认为自己就是黑客。他们使用这一词语来表示自己所展示的技艺和本领。系统侵入者不愿意将自己形容成“计算机入侵者”、“骇客”或“计算机破坏者”。这些词语由那些在传统上认为自己属于黑客的人们创造，但他们对玷污黑客这一“高贵”称号深恶痛绝，并公开进行强烈抵制。这种行为表现在将“黑客”一词用作计算机罪犯的同义词上，当然，这也是人之常情，也可以理解。然而，以上术语均未得到广泛认可。在某种程度上，惟一被接受的术语是“计算机朋客”（cyberpunker）——不过它也并未被主流媒体所接受。

① “Q&A with Emmanuel Goldstein of 2600: The Hacker's Quarterly,” CNN Online, April 1999