科海电脑技术丛书

黑客就这么几招

阎　雪　编著　第2版

你害怕电脑被黑客入侵吗？
你清楚黑客如何进行攻击吗？
你知道如何避免被黑吗？
从黑客的历史、技术的演进、入侵的过程及防护，彻底剖析黑客的原貌

Hacker Technology

北京科海集团公司　出品

科海电脑技术丛书

黑客就这么几招

(第2版)

阎　雪　编著

你害怕电脑被黑客入侵吗?
你清楚黑客如何进行攻击吗?
你知道如何避免被黑吗?
从黑客的历史、技术的演进、入侵的过程及防护，彻底剖析黑客的原貌

北京科海集团公司 出品

内 容 简 介

本书从黑客攻击的角度出发，全面、详尽地介绍了黑客的种种攻击技术。书中对每种攻击方法都附有攻击实例，其中大部分攻击实例是从未公开过的；在介绍各种攻击方法的同时都给出了相应的用户对策，使广大网民和网络管理员可以保障自己系统与信息的安全，完善自己的网络环境。

本书的第1版在国内是畅销书，并且被台湾松岗电脑图书资料股份有限公司以繁体中文在台湾出版。自第1版畅销后，又有许多崭新的工具和技术出现，第2版在尽量保留第1版精华内容的基础上，加入了一些新的技术资料以及新近发生的重要黑客事件，并对本书所附光盘的相应软件作了更新。

本书适合计算机网络管理员、系统维护人员、网络用户、计算机爱好者以及大专院校有关专业的师生阅读参考。

注意：光盘中的工具软件仅用于实验的目的，其宗旨是让您认识黑客，了解其攻击手段，从而防范黑客的非法攻击。若使用本光盘中的工具进行恶意破坏，必将受到社会的谴责和法律的制裁！

书　　名：黑客就这么几招（第2版）
作　　者：阎　雪
责任编辑：张　律
出　　品：北京科海集团公司
印 刷 者：北京市耀华印刷有限公司
发　　行：新华书店总店北京科技发行所
开　　本：787×960　1/16　印张: 38. 125　字数：601千字
版　　次：2002年3月第2版　2002年4月第2次印刷
印　　数：5001~8000
盘　　号：ISBN 7-89998-022-4
定　　价：55.00 元（1CD）

第二版前言

随着因特网在中国的进一步发展，网络安全技术也显得越发重要了。在《黑客就这么几招》(2000年12月第1版) 出版后一年的时间中，网络安全攻击以及防卫技术都有了显著的发展。例如，最近有一种被怀疑是国人编写的网络蠕虫病毒——"红色代码"在全球流行，被攻击的机器数以万计，这种病毒就使用了多种当今最先进的网络编程技术。

为了使广大网络用户以及网络管理员能够了解当今最新的网络攻击和防卫技术的发展情况，《黑客就这么几招》推出了第二版。在第二版中除了删除了第一版中基础知识的介绍部分以外，尽量保留了上一版的精华内容，并加入了一些新的技术资料以及最近发生的重要黑客事件。

新增加的内容主要包括：第1章中的"2000年中美黑客大战记实"、第5章"如何控制普通用户的计算机"、第6章中的"Windows下的溢出以及格式化串溢出"、第8章中的"X-Scanner介绍"、第14章"高级攻击技巧"以及第15章"攻击的善后工作"。

除了加入新内容外，还对书中介绍的一些软件进行了版本更新，使读者能够了解最新版本软件的新功能以及新特点。同时，本书附带的光盘中的相应软件均更新为最新的版本。

本书第二版在组织结构上仍然分4个部分，并对某些章节的顺序进行了调整，以便读者能够更好地理解其中的内容：

第1部分主要介绍黑客的历史、行为准则以及2000年中美黑客大战始末经过，包括第1章"黑客的历史"。

第2部分主要介绍黑客对普通用户的攻击手段，包括第2章"计算机病毒"、第3章"特洛伊木马"、第4章"网络炸弹"和第5章"如何控制普通用户的计算机"。

第3部分是本书的重点，主要介绍黑客对网站和网络的攻击手段。包括第6章"缓冲区溢出"、第7章"网络攻击的一般步骤及实例"、第8章"扫描器"、第9章"

密码破解"、第10章"sniffer"、第11章"利用Web进行攻击"、第12章"拒绝服务攻击"、第13章"欺骗攻击"、第14章"高级攻击技巧"、第15章"攻击的善后工作"和第16章"常见的系统漏洞及攻击实例"。

第4部分对网络安全防护体系的一些组成部分做了简要介绍，包括第17章"数据加密技术"、第18章"防火墙技术"和第19章"入侵检测系统"。

鉴于计算机技术的飞速发展，书中所述难免有不当之处，欢迎广大读者多提意见和建议，指出错误和不足。

编者

2001年11月

第一版前言

随着因特网的日益普及，上网对于许多人来说已经成为生活中必不可少的一部分，新老网民们通过网络来查找资料、交流信息。对于企业而言，网络更是占有举足轻重的地位，电子商务已经有逐步取代传统企业经营方式的趋势。但网络在带给我们极大便利的同时，也带来了另外一个棘手的问题，就是"黑客"问题。

由于因特网本身的设计缺陷及其开放性，使其极易受到黑客的攻击。根据美国有关安全部门统计，因特网上98%的计算机受到过黑客的攻击性分析，50%的机器被黑客成功入侵，而被入侵机器中有20%的管理员尚未发现自己已经被入侵。网络的安全性已经成为阻碍因特网在全球发展的重要因素之一。最近，美国包括"雅虎"、"亚马逊"、CNN在内的一些著名网站遭到黑客的大规模袭击，蒙受了巨大经济损失，引起了全世界对网络安全的密切关注。越来越多的人意识到，黑客已经成为全球新的公害，必须采取有力措施保护网络免受其扰。

在许多人眼中，"黑客"是一些高深莫测的神秘人物，他们利用手中所掌握的技术肆意攻击网站、盗取商业机密。加上一些媒体对黑客事件不负责任的夸大报道，使得黑客以及黑客技术对大多数普通网民而言更多了一层神秘面纱。其实，黑客以及黑客技术并不神秘，也并不高深。一个普通网民在具备了一定基础知识之后，就可以成为一名黑客，甚至无须任何知识，只要学会使用一些黑客软件，同样可以对网络实施攻击，这也正是如今网络攻击如此盛行的原因之一。

俗话说，"知己知彼，百战不殆"。想要更好地保护自己不受黑客的伤害，就必须对黑客技术有一定的了解。只有对黑客的种种攻击手段有了详尽的认识，才能进行更有效、更具针对性的防护，使自己免受黑客攻击。我们本着使中国广大网民"认识黑客，了解黑客、防御黑客"的原则编写了这本书，从攻击技术的角度对黑客的种种手段作了详尽的介绍，目的在于让普通网民以及网络管理员对黑客技术有一个大致的了解，从而能够保护自己免受伤害，或把损失降低到最小程度。需要强调的是，黑客行为是违反我国有关法律规定的，如果对别人实施攻击并造成了损失，就必须对自己的

行为负法律责任。基于上述原因，本书在每介绍一种攻击手法的同时，都会给出与之相对应的详尽的防护方法，希望读者能够善用本书。

本书的重点在于介绍黑客的攻击手段和提供相应的保护措施，在组织结构上共分四个部分：

第1部分主要介绍黑客的历史、行为准则以及相关的基础知识，包括第1章"黑客的历史"和第2章"基础知识介绍"。

第2部分主要介绍黑客对普通用户的攻击手段，包括第3章"计算机病毒"、第4章"特洛伊木马"和第5章"网络炸弹"。

第3部分包括第6章"网络攻击的一般步骤及实例"、第7章"扫描器"、第8章"缓冲区溢出"、第9章"密码破解"、第10章"sniffer"、第11章"利用Web进行攻击"、第12章"拒绝服务攻击"、第13章"IP欺骗攻击"和第14章"常见的系统漏洞及攻击实例"。这一部分主要介绍黑客对网站、网络的攻击手段。

第4部分对网络安全防护体系的一些组成部分做了简要介绍，包括第15章"数据加密技术"、第16章"防火墙技术"和第17章"入侵检测系统"。

由于作者本人水平有限，加之时间仓促，书中难免有不当之处，还望广大读者多提宝贵意见。

编者

2000年11月

目 录

第1部分 基 础 知 识

第2部分 攻击普通用户

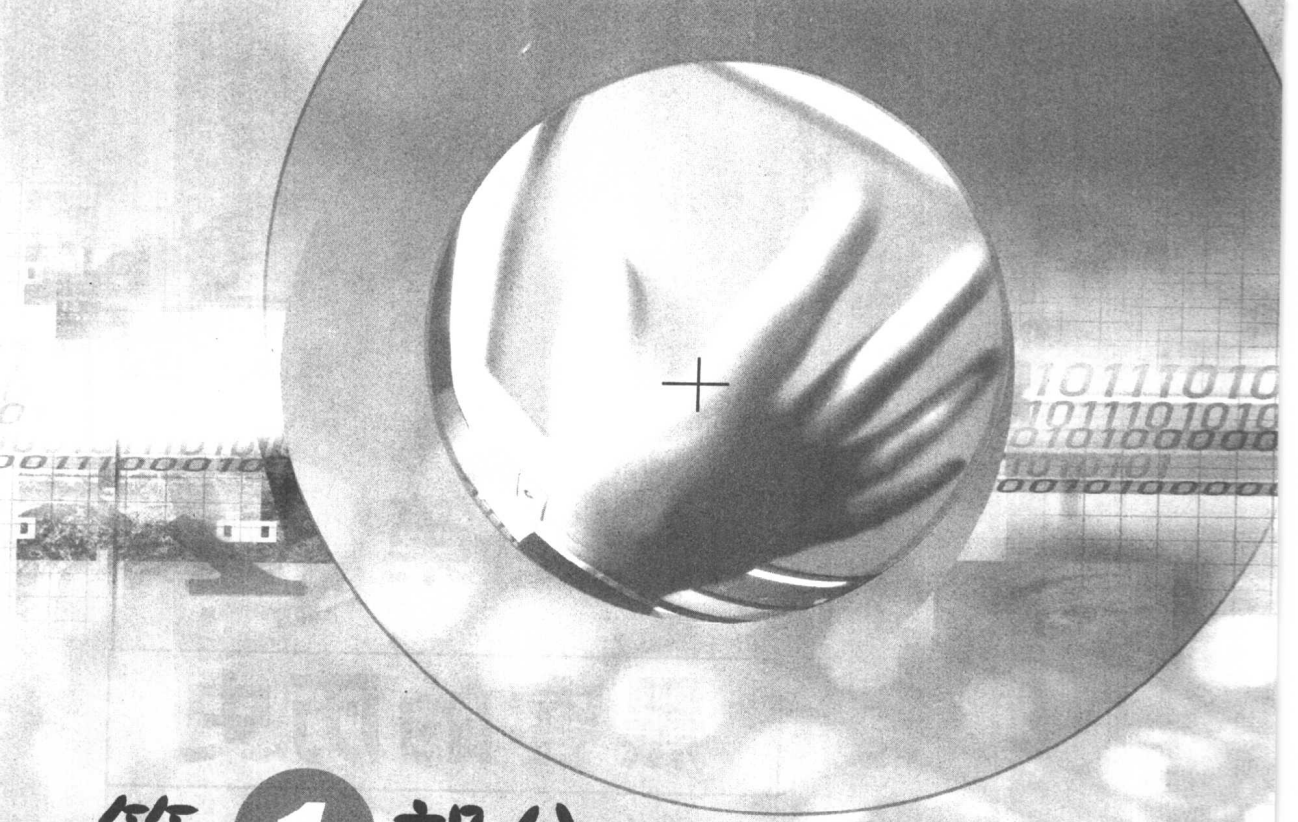
第3部分 攻击网络与网站

目 录

第4部分 网络安全防护

目 录

附 录



第 1 部分

基础知识

- 黑客的历史