信息安全大系

- 精选近100个攻防示例，帮助读者提升实战能力
- 涵盖脚本注入、远程控制、后门、扫描、嗅探、黑客编程、社会工程学等主流的攻防技术
- 完整的攻防实战案例：揭秘黑客入侵过程，提供系统加固策略

黑客攻防
实战秘技

傅奎 编著

人民邮电出版社
POSTS & TELECOM PRESS

傅奎 编著

黑客攻防

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客攻防实战秘技 / 傅奎编著. —北京：人民邮电出版社，2009.7
ISBN 978-7-115-20685-5

Ⅰ. 黑… Ⅱ. 傅… 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（2009）第050126号

内 容 提 要

本书是指导读者学习如何防御黑客攻击的实战书籍。书中结合当前互联网上主流的防范黑客攻击的技术，详细地介绍了读者在防范黑客攻击时必须掌握的基本知识、实用工具和技巧，对读者在防御黑客攻击时经常遇到的问题给予了专业性的解答，并通过实战案例给读者讲述了多种防范技术的具体应用。

全书分为四篇共 21 章，主要内容包括，网络安全基础知识、系统漏洞扫描、搜索引擎信息利用、操作系统本地攻防、网络封锁与代理突破、木马后门防御、网络抓包嗅探、欺骗攻击防御、SQL 注入防御、XSS 跨站脚本攻击防御、缓冲区溢出、防火墙、社会工程学、系统安全加固等知识。

本书采用大量真实案例，内容新颖，实例丰富，语言通俗易懂。书中内容都与当前网络安全现实结合紧密，既包括有主流的技术，也探讨了许多前沿知识，通过本书的学习将会很好地提高读者防范黑客的水平。

本书内容丰富，实战性和可操作性强，适合于网络安全技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习用书和参考资料。

黑客攻防实战秘技

◆ 编　　著　傅　奎
责任编辑　屈艳莲
执行编辑　张　涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：21.25
字数：505 千字　　2009 年 7 月第 1 版
印数：1－3 500 册　　2009 年 7 月河北第 1 次印刷

ISBN 978-7-115-20685-5/TP

定价：39.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前言

伴随着网络技术的高速发展，信息安全问题已日益受到人们的关注。信息安全尤其是网络安全，已涉及社会的方方面面，这其中的黑客防范是最值得普及的技术。本书以此为切入点，通过从理论到实践的方式，为读者介绍了当前互联网上流行的各种防范黑客攻击的技术。

本书内容

为了使读者能够逐步掌握全书内容，本书共分 4 篇：网络安全技术基础篇、木马、嗅探和后门防范技术篇、网络防范技术篇和防范案例实战篇。

网络安全技术基础篇（第 1 章～第 6 章）。介绍当前网络安全现状、操作系统安全使用策略、网络协议、常用防范软件、防范黑客编程等。为了提高读者的学习兴趣，讲解上以简单生动的例子介绍一些比较实用的攻防技巧。

木马、嗅探和后门防范技术篇（第 7 章～第 13 章）。通过大量的实例，介绍了当前主流的木马、嗅探和后门防范方法。主要内容为，搜索引擎信息获取技术、漏洞扫描、操作系统本地攻防、网络封锁与代理突破、木马与后门防范技术、网络嗅探等。其中搜索引擎信息获取技术是当前网络攻防中热门话题，本篇中做了系统的阐述。

网络防范技术篇（第 14 章～第 19 章）。本篇主要介绍网络上最为流行和成熟的防范手段。主要内容为，SQL 注入攻击防御、跨站脚本攻击防御、缓冲区溢出、欺骗攻击防御、社会工程学、防火墙技术及综合防范技术运用等。

防范案例实战篇（第 20 章～第 21 章）。为了把前面的知识有一个综合的应用，本篇结合个人实战经验，讲述了一个揭秘黑客攻防过程的综合案例，以及一个如何加固系统安全的防御案例，是整本书的知识总结和实战技能提升部分。

本书特点

本书探讨黑客攻防时不仅仅停留在技术上，更多地是倡导学习网络安全技术，增强网络安全意识，提升我国计算机网络安全的整体水平。读者在学习的同时，也应遵守职业准则和国家相关的法律法规。

本书的特点主要体现在以下几个方面。

- 本书的编排采用循序渐进的方式，适合初学者由浅入深地学习网络安全知识。通过全书 21 章的学习，读者可以掌握当前网络上主流的黑客防范技术。
- 本书介绍的各种攻防技术不仅体现在技术实现上，而且从原理角度对技术进行了阐

述。通过本书的学习，读者能够更加深入地理解防范黑客技术的真实原理，如书中提到的SQL 注入漏洞的具体表现、漏洞产生原理及防范方法。

- 本书注重理论结合实际，相关案例更是贴近真实环境。如书中提到的通过 SSH 加密隧道突破网络封锁登录 QQ、办公室 MSN 聊天加密、构筑铜墙铁壁安全系统等。
- 本书在介绍大量网络安全技术实现原理及具体应用时，均提供了典型的案例和参考图例。读者通过书中提供的真实场景的截图，能够快速学习和掌握各类攻防技术，以便在学习上少走弯路，如书中图文并茂地讲述了开发 Bug 提交系统的安全测试等。
- 本书讲解的内容与当前网络安全现实相结合，既有主流的技术知识，也涉及部分前沿技术，如书中提到的社会工程学等知识。

读者对象

- 网络安全入门者；
- 网络安全爱好者；
- 网络安全管理员。

致谢

本书稿的完成得到了许多人的支持，在此一并致谢。感谢北京的 LXJ 朋友，他给我写作提供了很大的帮助；感谢我的朋友“月亮”，他的多次鼓劲使我能够在面临困境时咬牙向前；感谢融智科技的陈冠军朋友，她的热情帮助和耐心指导一直在鼓舞着我努力写作。

在写作过程中，我力求精益求精，但由于时间所限，书中难免存在一些不足之处，敬请广大读者批评指正。如果您在使用本书时遇到问题，可以发邮件到 zhangtao@ptpress.com.cn 与我们联系。

编者

目录

第一篇　网络安全技术基础篇

第三篇 网络防范技术篇

第四篇 防范案例实战篇

第一篇

网络安全技术基础篇

- 第 1 章　知己知彼，百战不殆——网络安全现状
- 第 2 章　千里之行始于足下——认识操作系统及安全策略
- 第 3 章　网络核心基础——网络协议
- 第 4 章　工欲善其事，必先利其器——安全利器
- 第 5 章　自力更生——编程防范黑客
- 第 6 章　牛刀小试——防范入侵实战演练

第1章 知己知彼，百战不殆——网络安全现状

本章主要为了配合后面内容的讲解，让读者先对网络安全有一个全面的认识。内容涉及：黑客的由来及其发展现状、国内外网络安全的现状、日益猖獗的互联网犯罪和国家出台的相关法律、法规。

1.1 网络安全现状及发展趋势

我国的互联网起步较晚，虽然经过多年的发展已经有了很大进步，但是仍然存在很多问题，尤其是基础设施较差、核心技术级的关键人员缺乏等。最新统计显示，我国拥有网民两亿多人，位居世界第二。面对如此庞大的用户群，我们不得不去考虑日益严峻的网络信息安全现状。

1.1.1 认识黑客

“用了好几年的 QQ 号被盗！”
“苦练了 50 级的传奇游戏账号中的装备一夜之间被卸光！”
“XX 媒体报道，重要的网站遭遇黑客入侵！”
“HD-DVD 最新加密技术被黑客瞬间破解！”
“熊猫烧香病毒感染我的机器啦！”
……

上面的场景相信很多人都遇到过。大多数上过网的读者，或多或少地接触过黑客这个词。黑客的英文原名叫“Hacker”，本意是指那些热衷解决问题、克服限制的技术人员。不过由于近年计算机领域的飞速发展，也在不断地创造黑客的传奇，使得黑客常被理解为计算机高手。同时，伴随着互联网犯罪的扩大化，很多人更是将黑客理解为攻击或入侵计算机的人员。

1.1.2 互联网安全现状

当前，计算机病毒、各种有害信息、系统安全漏洞和网络违法犯罪等信息安全问题日渐

突出，这不仅与信息通信业的持续健康发展目标相背，也给用户使用互联网带来了许多负面影响。因此，互联网信息安全状况受到了社会各界的关注和重视。

互联网犯罪是近几年媒体关注的热门话题。从“传奇大盗”到“熊猫烧香”，短短几年的时间，网络犯罪活动越来越猖狂。

网络犯罪其根本原因是，某些人希望通过计算机用非法手段获取利益，如一些虚拟的网络游戏中，黑客们利用非法手段盗取他人账号、密码，再通过一定的渠道将盗来的装备或虚拟货币在市场上兜售非法获利。

另外一方面原因是，一些网民在上网时缺乏防范黑客攻击的安全意识，如果用了盗版的操作系统，而且没有下载修复系统漏洞的各种升级程序，这样“千疮百孔”的计算机一旦连接上网络就很容易被黑客种植木马或病毒，成为黑客手中的“肉鸡”。

提示：“肉鸡”是指那些被植入木马或后门程序后，完全受黑客控制的计算机。形象地比喻为黑客菜板上的“肉鸡”，任人宰割。

一些黑客组织从未放弃对我国计算机网络进行攻击渗透，从 CNCERT 的统计报告可以看出，每天国内网站被入侵的数目居高不下，如图 1.1 所示。

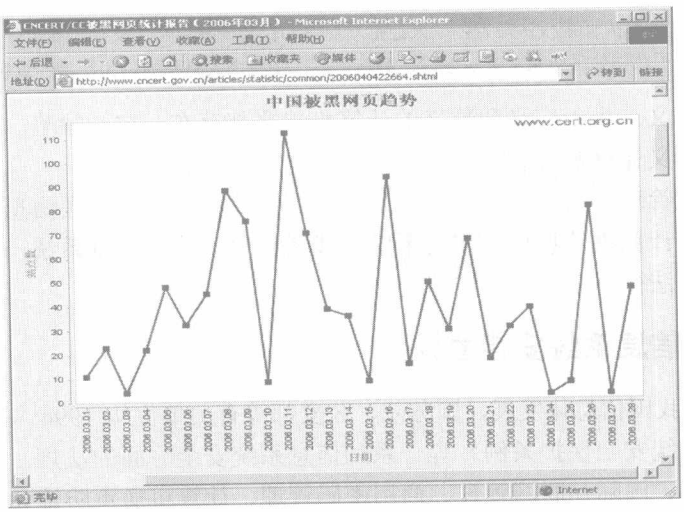

图 1.1 CNCERT 统计的网站被入侵情况

1.1.3 黑客技术发展

当前网络上各种常见的攻击技术包括：漏洞扫描、口令破解、脚本注入、缓冲区溢出、网络嗅探、木马后门、病毒破坏、代理渗透、身份伪造、社会工程学等。

随着黑客工具的傻瓜化，使得很多本身技术并不是很高的人也能很快上手，并能用这些工具制造出一定的破坏。据统计，网络上绝大部分所谓的黑客攻击实际上是那些并没有掌握多少深层技术的“菜鸟黑客”所为，他们常被称为“Tool User”。

由于信息网络的迅速发展，新的黑客攻防技术已经不再是简单入侵和破坏，而是上升到从系统的角度对目标系统造成破坏和保护己方系统稳定运行的高度。

1.2 计算机犯罪及相关法律

本节以计算机犯罪为基础，介绍计算机犯罪相关的概念、特点、防范及国家相关法律、法规。

1.2.1 计算机犯罪相关概念

由于计算机普及率的提高，人们利用计算机从事的各项活动日益增多。那么在计算机中什么样的活动是合法的，什么样的活动是非法的，存在一个法律界限的问题。计算机犯罪作为人类社会的一种新兴犯罪形式，人们对它的认识或多或少存在一定的局限性。

（1）广义的计算机犯罪定义。在计算机犯罪出现的早期，由于计算机应用面较窄，计算机技术较为神秘，人们把与计算机相关的犯罪都认定为特殊犯罪，均归为计算机犯罪。

（2）狭义的定义。针对广义的计算机犯罪定义过于宽泛，各国学者和机构都提出了自己冠以计算机犯罪定义的观点。

说明：瑞典的私人保密权法规定：“未经批准建立和保存计算机私人文件，有关侵犯受保护数据的行为，非法存取电子数据处理记录或非法修改、删除记录，侵犯个人隐私的行为都是计算机犯罪”。

（3）折中的定义。由于广义和狭义的计算机犯罪都存在一定的缺陷，很多人开始寻求一种折中的方式来定义计算机犯罪。

公安部计算机管理监察司给出的定义是：所谓计算犯罪，就是在信息活动领域中，利用计算机信息系统或计算机信息指示作为手段，或者针对计算机信息系统，对国家、团体和个人造成危害，依据法律，应当予以刑罚处罚的行为。

1.2.2 计算机信息系统安全立法

为适应和保障我国信息化发展，国务院、公安部等有关单位从 1994 年起颁发了《中华人民共和国计算机系统安全保护条例》等一系列信息系统安全方面的法规。这些法规主要涉及信息系统安全防护、国际互联网管理、商用密码管理、计算机病毒防治和安全产品检测与销售 5 个方面。

1.3 小结

本章通过较短的篇幅为读者介绍了黑客的由来、国内外网络安全现状及发展趋势，同时还介绍了计算机犯罪相关的法律知识。从下一章开始，将介绍相关技术的理论知识，为读者后续学习打下基础。

第2章 千里之行始于足下——认识操作系统及安全策略

操作系统（operating system）是所有软件和系统运行的基础，它是一个大的基础平台。软件、系统都是围绕操作系统而发挥作用。网络安全也包括系统安全，因此学习网络安全，认识操作系统是必不可少的一个环节。本章的出发点是，在读者学习网络安全之前，为读者介绍一些必备的操作系统知识。在了解操作系统的各种特性（尤其是安全机制），后期的学习才能更加深入和透彻。

2.1 Windows 操作系统

Windows 操作系统在个人桌面操作系统用户中占有相当高的比率。由于 Windows 操作系统拥有最多的个人用户，Windows 操作系统也是黑客们紧盯的对象。本节将从注册表、系统服务、文件格式、安全机制等方面介绍 Windows 操作系统的相关知识。在后面章节介绍的 Windows 平台下的攻防技术都将会涉及本节的内容。

2.1.1 认识注册表

注册表是 Windows 系统的核心，它控制着 Windows 整个系统的运行。注册表到底是什么？本小节将对这个问题展开全面的讨论，并为读者进一步操作注册表打下基础。

注册表（registry）是 Windows 系统的一个核心数据库，它是辅助 Windows 控制硬件、软件、用户环境和 Windows 界面的一套数据文件。注册表包含系统的所有应用程序和软、硬件的相关信息。从用户的角度看，注册表系统由注册表数据库和注册表编辑器两部分组成。

提示： 操作系统 Windows 目录下的 regedit.exe 就是注册表编辑器。在 Windows 早期的版本中（Windows95 以前），这些功能是靠 WIN.INI、SYSTEM.INI 及其他与应用程序有关联的.INI 文件来实现的。

在 Windows 系列的操作系统中，文件 SYSTEM.INI 和 WIN.INI 包含了操作系统所有的控制功能和应用程序的信息，其中 SYSTEM.INI 负责管理计算机硬件，而 WIN.INI 则管理桌面和应用程序。系统中所有驱动、字体、设置和参数都会保存在.INI 文件中，任何新程序都会被记录在.INI 文件中，这些记录可以在程序中被引用。由于受到 WIN.INI 和 SYSTEM.INI

文件大小的限制，一般由程序员添加辅助的 INI 文件以便用来控制更多的应用程序。举例来说，某个软件 SoftX 安装成功后会生成 softx.ini 文件，它包含有选项、设置、默认参数和其他关系到该程序正常运行的信息。在操作系统的 SYSTEM.INI 和 WIN.INI 中只需指出 softx.ini 的路径和文件名即可。

在早期的 Windows 版本中，SYSTEM.INI 和 WIN.INI 控制着所有系统自身和应用程序的特征和存取方法，它在少数的用户和少数应用程序的环境中工作得很好。随着应用程序的数量和复杂性的增加，则需要在.INI 文件中添加更多的参数项，这样每当有新的程序安装后操作系统都会去变更.INI 文件。但是，很少有程序在卸载后会清理这个配置文件，导致 SYSTEM.INI 和 WIN.INI 这个两个文件会变得越来越大，增加的内容会导致系统性能越来越慢。而且当应用程序需要升级时将会遇到很多麻烦问题，升级会增加更多的参数项，而对于旧的参数则很少修改。由于.INI 文件的大小最多不超过 64kB，因此这会严重影响系统性能。为了解决这个问题，软件提供商一般都会提供自己的.INI 文件，然后指向特定的 INI 文件，如 WIN.INI 和 SYSTEM.INI 文件，这样会使多个.INI 文件影响系统正常的存取级别设置。如果一个应用程序的.INI 文件和 WIN.INI 文件在参数设置上发生冲突，程序往往无法判断其优先级别。

注册表是一套控制操作系统外壳和辅助系统响应外来事件工作的文件。这些外来“事件”的范围包括：直接访问硬件设备或者接口，如何响应特定用户，应用程序及运行等。注册表因为其复杂性，被设计为专门向 32 位应用程序提供服务，其文件大小被限制为约 40MB。

2.1.2 注册表和 INI 文件的区别

在 Windows XP 下，注册表和 Windows NT 以前的 INI 文件主要有以下几点不同。

- 注册表采用了二进制形式登录数据。
- 注册表支持子键，每一个子关键字拥有自己的数据。
- 注册表中的键值项可以包含可执行代码，而不是简单的字符串。
- 注册表可以存储系统中多个用户的配置信息。

Windows 系统在安装过程中，安装程序会扫描计算机的硬件配置，并扫描检测系统中硬件的驱动，然后用扫描结果初始化注册表。同时，安装程序在系统盘的根目录下生成 System.1st 文件。如果系统更换了部分硬件，而这些硬件的驱动在注册表中没有存储，那么计算机用户就需要重新安装操作系统。

说明： System.1st 是注册表的原始备份文件。

下面通过对 Windows 系统工作过程的跟踪性描述，揭示操作系统如何使用注册表来启动计算机。

（1）启动计算机。启动时，Windows 系统自动扫描计算机的硬件配置，并将扫描结果写入注册表，扫描结果包括 CPU 数量，内存容量等配置信息。同时，系统更新每台设备的相关信息，包括设备所使用的资源（DMA 中断和 I/O 地址），然后，Windows 系统利用注册表来配置计算机。

说明： 配置过程主要包括初始化设备驱动程序，打开计算机的网络连接，以及启动相关的服务，如任务表等。