

现用现查红宝书随身易

必备电脑工具书

黑客攻防 与网络安全速查

张增强 编著



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客攻防

与网络安全速查

张增强 编著



中国铁道出版社

2004·北京

内 容 简 介

在互联网时代，每一个连接到网络上的计算机都面临着被攻击的威胁。本书目的在于让读者了解黑客的攻击手段，使读者在实际应用中碰到黑客攻击的时候，能够做到“心中有数”，本书主要讲解了计算机攻防知识、操作系统攻防、IE 攻防、QQ 攻防、电子邮件攻防、冰河木马攻防、数据包拦截以及杀毒和防火墙技术等内容。

本书适合广大计算机爱好者和网络冲浪者使用，同时对系统管理员也有参考价值。

图书在版编目 (CIP) 数据

黑客攻防与网络安全速查/张增强编著. —北京: 中国铁道出版社, 2003. 10

(现用现查红宝书随身易: 5)

ISBN 7-113-05548-6

I. 黑… II. 张… 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 092760 号

书 名: 黑客攻防与网络安全速查

作 者: 张增强

出版发行: 中国铁道出版社 (100054, 北京市宣武区右安门西街 8 号)

策划编辑: 严晓舟 郭毅鹏

责任编辑: 苏 茜 赵树刚

封面设计: 孙天昭

印 刷: 北京市兴顺印刷厂

开 本: 787×1092 1/64 印张: 6.75 字数: 206 千

版 本: 2003 年 11 月第 1 版 2004 年 3 月第 2 次印刷

印 数: 6001~11000 册

书 号: ISBN 7-113-05548-6/TP·1050

定 价: 全套丛书定价 80 元 (共 8 册)

版权所有 侵权必究

凡购买铁道版的图书, 如有缺页、倒页、脱页者, 请与本社计算机图书批销部调换。

丛书序

现在计算机发展可谓一日千里,已经从昔日的“阳春白雪”变成了人们日常用的一门工具。面对人们学习电脑的热情,我们一直在思考这样的问题:读者们(特别是初、中级电脑用户)到底需要什么样的电脑书籍呢?什么样的书能够用最实用的语言、最优惠的价格、最精美的效果来引导读者进入广阔的天地呢?什么样的书能够让有一定电脑基础的用户(希望在更短的篇幅里容纳更多的内容的人)也爱不释手呢?

为此,我们策划了这套小红宝书系列,目的是:希望用户拿到手就能用,按照书中的步骤一步步操作就能实现想要的效果,同时避开深奥知识的讲解,直接告诉读者如何做,让读者在操作过程中体会电脑的奥妙。本丛书的特点总结如下:

(1) 知识全面、覆盖面广。争取把常用的东西都讲到。

(2) 结构清楚、步骤详细。所有的章节、步骤都尽量细化,目录也做得很详细,让读者可以轻松查阅本书内容。

(3) 动手操作、实例引导。用一步步的实际操作来引导读者，让用户亲自在动手的过程中掌握知识。

(4) 实惠精致、物有所值。我们竭尽所能把所有的细节做到位：排版更紧凑，印刷更精美，格式更细致，定价更合理。

希望更快地学习电脑知识吗？希望更轻松地深化电脑应用吗？不要死啃大块头的艰深知识了，拿起红宝书来，开始学习吧！

编者

2003.9

前言

九十年代初，互联网在全球迅猛发展，为人们提供了极大的方便、自由和无限的财富。同时，互联网也带来了一些负面影响，“信息垃圾”、“邮件炸弹”、“电脑黄毒”等越来越威胁到网络的安全。尤其是黑客攻击，随着互联网的普及，已成为威胁网络安全的最大隐患。

本书目的在于让读者了解黑客的攻击手段，使读者在实际应用中碰到黑客攻击的时候，能够做到“心中有数”，更重要的是，希望读者能够运用本书介绍的黑客攻击防守方法去防范黑客的攻击，使自己的网络更加安全。全书的主线是黑客的“攻与防”，每一章都是围绕“攻与防”来展开叙述的，做到“有攻有防”。

本书主要讲解了计算机攻防基础知识、操作系统攻防、IE 攻防、QQ 攻防、电子邮件攻防、冰河木马攻防、数据包拦截以及杀毒和防火墙技术等内容。

本书按照速查手册的格式来编排，便于快速查阅，提高读者的效率。

陈贤淑、陈晓娟、廖康良等参与了本书的编排工作。

编者

2003.9

目 录

第 1 章 计算机攻防基础知识	1
1-1 计算机系统漏洞概述.....	2
问题 1 什么是漏洞.....	2
问题 2 漏洞有哪几种.....	3
问题 3 什么是拒绝服务 (Denial of Service).....	5
问题 4 什么是脆弱的帐号和密码.....	6
问题 5 入侵电子邮件系统有几种方法.....	7
问题 6 什么是文件共享.....	8
问题 7 IIS (Internet Information Server) 有什么漏洞.....	9
问题 8 扫描器和常见的扫描器介绍.....	10
1-2 黑客的攻击手段和防御手段.....	13
问题 1 黑客如何进行主动攻击.....	14
问题 2 黑客被动攻击的方法.....	16
问题 3 防御黑客攻击有什么方法.....	18

第 2 章 Windows NT/Windows 2000

攻防	21
2-1 Windows 2000 简体中文版登录	
输入法漏洞	22
问题 1 如何利用 Windows 2000 简体 中文版登录输入法漏洞攻击	22
问题 2 Windows 2000 简体中文版登录 输入法漏洞的修补	30
2-2 Windows 2000 系统崩溃漏洞	36
问题 1 利用 Windows 2000 系统崩溃 漏洞进行攻击	36
问题 2 Windows 2000 系统崩溃漏洞 的修补	39
2-3 Windows NT/Windows 2000 SAM 数据库 安全隐患	39
问题 1 什么是 SAM	39
问题 2 利用 Windows NT/Windows 2000 SAM 数据库安全隐患 进行攻击	41
问题 3 消除 Windows NT/Windows 2000 SAM 的安全隐患	42
2-4 获取 Windows NT/Windows 2000	

当前登录用户的密码.....	43
问题 1 利用 Win2kPass 获取 Windows NT/ Windows 2000 当前登录用户 的密码	43
问题 2 防止 Windows NT/Windows 2000 当前登录用户的密码被获取	46
第 3 章 IE 攻防	47
3-1 利用网页恶意修改系统.....	48
问题 1 什么是万花谷病毒	48
问题 2 对万花谷病毒恶意修改的修复 和防御方法	52
3-2 IE 炸弹	62
问题 1 IE 窗口炸弹攻击.....	62
问题 2 IE 窗口炸弹的防御.....	66
问题 3 IE 共享炸弹的攻击.....	69
问题 4 IE 共享炸弹的防御.....	70
3-3 利用网页删除硬盘文件攻击.....	71
问题 1 利用 Office 对象删除硬盘文件 的攻击	71
问题 2 利用 Office 宏删除硬盘文件 的攻击	73
问题 3 利用 ActiveX 对象删除硬盘	

文件的攻击	80
问题 4 防止硬盘文件被删除	83
第 4 章 QQ 攻防	87
4-1 在 QQ 中显示对方 IP 地址	88
问题 1 如何在 QQ 中显示对方 IP 地址	88
问题 2 如何在 QQ 中不让对方得到 自己的 IP 地址	91
4-2 QQ 密码的非在线破解	97
问题 1 如何使用 OICQ 密码瞬间 破解器	97
问题 2 对于 OICQ 密码瞬间破解器 的防范	100
问题 3 使用 QQ 木马窃取 QQ 2000 密码	101
问题 4 防范 QQ 木马的方法	104
4-3 QQ 密码在线破解	106
问题 1 如何利用 QQPH 在线破解 王破解 QQ 2000 密码	107
问题 2 用天空葵 QQ 密码探索者 破解 QQ 2000 密码	114
问题 3 用 QQExplorer 破解 QQ 2000 密码	121

问题 4	对 QQ 密码在线破解的防范.....	129
4-4	QQ 消息炸弹	134
问题 1	发送 QQ 2000 消息炸弹.....	134
问题 2	向指定的 IP 地址和端口号 发送 QQ 2000 消息炸弹.....	140
问题 3	对 QQ 2000 消息炸弹的防范.....	141
第 5 章	电子邮件攻防.....	143
5-1	入侵电子邮箱.....	144
问题 1	Emailcrack 窃取电子邮箱密码.....	144
问题 2	黑雨——POP3 邮箱密码暴力 破解器的使用方法	147
问题 3	溯雪 Web 密码探测器的 使用方法	151
问题 4	流光窃取邮箱的密码	168
问题 5	抵御电子邮箱入侵	175
5-2	电子邮件炸弹.....	175
问题 1	Kaboom! 邮件炸弹	176
问题 2	Haktek 邮件炸弹.....	183
问题 3	拒绝垃圾邮件	186
问题 4	拒绝巨型邮件	194
问题 5	邮件炸弹的克星 E-mail Chomper.....	195

5-3	利用 Outlook Express 漏洞进行攻击.....	199
问题 1	Outlook Express 邮件欺骗	199
问题 2	Outlook Express 邮件欺骗 的防范	211
问题 3	如何利用附件中的 TXT 文件 进行攻击	212
问题 4	识别和防范隐藏扩展名的 TXT 文件进行攻击的方法	217
问题 5	识别和防范恶意碎片文件攻击 的方法	218
第 6 章	木马攻防	221
6-1	木马简介.....	222
问题 1	木马是如何侵入的	222
问题 2	木马入侵有几种常见方法	224
问题 3	木马是如何工作的	226
6-2	伪装木马程序.....	226
问题 1	用 Joine 文件合成工具 伪装木马	227
问题 2	用 ExeJoiner 文件合成工具 伪装木马	229
6-3	Back Orifice 2K 木马	232
问题 1	什么是 Back Orifice 2K 木马.....	232

目 录

问题 2	如何配置 BO2K 服务器端.....	232
问题 3	如何设置 BO2K 客户端.....	239
问题 4	如何检测 BO2K	243
问题 5	如何清除 BO2K	246
6-4	网络公牛 (Netbull) 木马.....	247
问题 1	配置网络公牛服务器端程序.....	247
问题 2	如何使用网络公牛客户端.....	251
问题 3	如何检测网络公牛.....	265
问题 4	如何手工清除网络公牛.....	267
问题 5	如何清除网络公牛服务器端.....	271
6-5	冰河木马.....	273
问题 1	冰河服务器端程序配置.....	273
问题 2	如何使用冰河客户端实现 远程监控.....	280
问题 3	冰河的检测.....	283
问题 4	使用冰河客户端程序删除 冰河木马.....	284
问题 5	手工删除冰河木马.....	286
第 7 章	数据包攻防.....	291
7-1	Unicode 漏洞攻防.....	292
问题 1	什么是 Unicode.....	292
问题 2	使用 RangeScan 查找	

	Unicode 漏洞.....	292
问题 3	利用 Unicode 漏洞简单修改 目标主机主页的攻击.....	300
问题 4	如何查看主机上的任何目录.....	306
问题 5	显示文件内容.....	308
问题 6	如何删除文件.....	309
问题 7	如何复制文件的同时将该 文件改名.....	310
问题 8	复制文件到另外的文件夹.....	312
问题 9	查找某一路径下的文件.....	312
问题 10	Unicode 漏洞解决方案.....	314
7-2	局域网数据包拦截.....	316
问题 1	使用 Sniffer Pro LAN 拦截 局域网数据包.....	316
问题 2	使用 Spynet 拦截局域网数据包.....	331
问题 3	局域网数据包拦截的防范.....	338
第 8 章	密码破解.....	341
8-1	破解“星号”密码.....	342
问题 1	什么是星号密码.....	342
问题 2	SnadBoy's Revelation 破解 “星号”密码.....	343
问题 3	Viewpass 破解“星号”密码.....	346

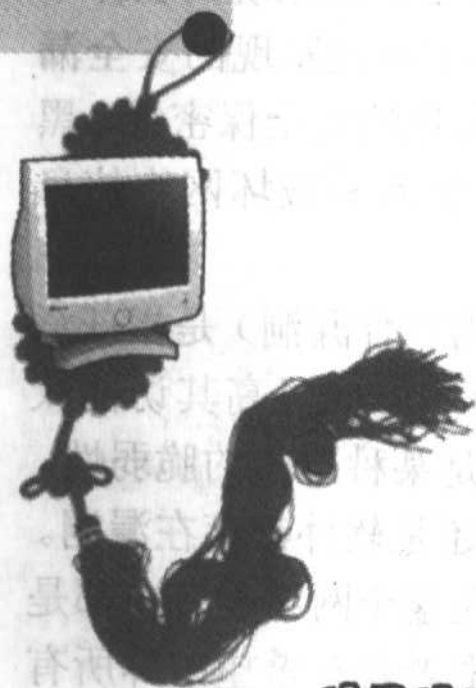
8-2	破解“ZIP”密码.....	347
问题 1	使用 Advanced ZIP Password Recovery 破解“ZIP”密码.....	348
问题 2	使用 Ultra ZIP Password Cracker 破解“ZIP”密码.....	354
8-3	破解“屏幕保护程序”密码.....	359
问题 1	使用 ScrSavPw 工具破解 屏保密码.....	359
问题 2	取消系统启动时的屏幕 保护程序.....	360
8-4	密码破解工具包 Passware.....	362
问题 1	破解“Office”密码.....	364
问题 2	破解“VBA”密码.....	367
8-5	如何选择安全的密码.....	372
问题 1	常见的危险密码有哪些.....	372
问题 2	密码的安全规则是什么.....	375
第 9 章	病毒防治.....	377
9-1	计算机病毒简介.....	378
问题 1	计算机病毒的特征.....	378
问题 2	计算机病毒的破坏.....	381
问题 3	计算机病毒防治的策略.....	383
9-2	金山毒霸.....	388

问题 1	金山毒霸有什么功能	388
问题 2	如何使用金山毒霸 2003 查杀病毒	389
问题 3	如何进行查毒设置	391
问题 4	当发现病毒时使用不同的 处理方式	393
问题 5	设置无法清除病毒时的 处理方式	394
问题 6	查毒结束后的处理方式	395
问题 7	如何使用 Office 安全助手	395
问题 8	如何使用 QQ、ICQ 安全助手	397
问题 9	如何使用病毒防火墙	399
9-3	防火墙技术	400
问题 1	什么是防火墙	400
问题 2	什么是天网防火墙	401
问题 3	如何设置安全级别	403
问题 4	设置应用程序规则	404
问题 5	如何定义自定义 IP 规则	406
问题 6	如何系统设置	408

CHAPTER

计算机攻防 基础知识

1



现用现查 **紅寶書** 隨身易