

HONG BAO SHU

电脑
COMPUTER

黑客攻防妙招

速查

宝典

红宝书编委会 编著



- ◎ 近1000条的攻击实例及防范技巧，内容丰富，覆盖面广。
- ◎ 操作步骤完整、详细，可即学即用，实用性强。
- ◎ 置于案头，随查随用，可方便您的工作，提高工作效率。

上海科学普及出版社

HONG BAO SHU

电脑
COMPUTER



TP393.198/102

黑客攻防妙招

速查

宝典

红宝书编委会 编著



上海科学普及出版社

图书在版编目 (CIP) 数据

黑客攻防妙招速查宝典 / 电脑红宝书编委会编著. —

上海: 上海科学普及出版社, 2008.8

ISBN 978-7-5427-3694-9

I. 黑... II. 电... III. 计算机网络—安全技术 IV. TP3.08

中国版本图书馆 CIP 数据核字 (2007) 第 146016 号

策划编辑 胡名正

责任编辑 林晓峰

黑客攻防妙招速查宝典

电脑红宝书编委会 编著

上海科学普及出版社出版发行

(上海中山北路 832 号 邮政编码 200070)

<http://www.pspsh.com>

各地新华书店经销

常熟市新骅印刷有限公司印刷

开本 787×1092

1/16

印张 23.75

字数 415000

2008 年 8 月第 1 版

2008 年 8 月第 1 次印刷

ISBN 978-7-5427-3694-9/TP·847

定价: 29.80 元

内 容 提 要

轻用其芒，动即有伤，是为凶器。

深藏若拙，临机取决，是为利器。

——《古剑铭》

黑客技术是一柄双刃剑，用法得当能够使自己的电脑更加安全，为广大用户提供更加多的有用的软件和信息；用法不当，就会对电脑用户和网络造成极大的危害。

针对现在网络上黑客和黑客软件泛滥的现状，本书从聊天工具、电子邮件、Web、蠕虫病毒、木马攻防以及系统漏洞防范、数据加密和备份这几个方面作了详细地介绍。本书收录了近1000条的攻击实例及防范技巧。在对每一实例进行合理客观分析的同时，给出了相应的解决方法和具体操作步骤，旨在帮助读者解决日常所遇到的黑客问题，并能掌握一定的对系统优化配置的技巧。

本书实例丰富、典型，内容新颖、翔实、通俗易懂，操作步骤详细明了，并附有要点提示。无论你的电脑是中了病毒，陷于苦恼，还是想要自己动手，为电脑构建一座“安全堡垒”，都能从本书中获益。

电脑红宝书编委会

主 编 蔡国钧

副主编 钱世德 崔亚海

编 委 罗振候 周红群 胡传国 杨万里

崔慧勇 太洪春 章五一 王 惠

庞志敏 薛淑娟 周清纯 黄 丹

戚 燕 瞿怡珉 刘 弘 忻 兵

前言

Foreword >>>

黑客，是广大电脑用户谈虎色变的一个名词。QQ、MSN 账号被盗，邮件中携带病毒，上网冲浪的时候中了病毒或者木马，导致自己的电脑无法正常工作，出现死机、蓝屏、主机无法启动、开机报警等现象，甚至自己的文件被莫名其妙地删除或者盗窃，这给用户正常的工作、学习和娱乐带来了很大的麻烦，甚至造成巨大损失。因此，对于一般的电脑用户，掌握一定的黑客防范技术是非常必要的。

但是现在网络信息的变化可以说是日新月异，黑客攻击手段也比以前更加隐蔽，这个对于很多专业的计算机人员来说都是比较困难的，在编写本书的时候，我们参阅了大量的相关文献和资料，收录了最常见的病毒或者木马的攻击实例和防范措施，编写了《黑客攻防妙招速查宝典》一书。书中对用户日常使用电脑时最大可能会碰到的黑客攻击以及网上泛滥最严重的病毒和木马给出了详细、可行、高效的解决方案，并且向用户介绍了多款口碑好的防毒软件和加密、数据备份软件的使用，使读者能在较短的时间内掌握电脑日常维护的相关知识，并能独立解决大多数在日常使用电脑时所遇到的各种黑客攻击问题。本书有如下几个特点：

☛ 内容丰富

本书收录了黑客攻击手段、防范措施、防火墙软件、聊天工具攻防、邮件攻防、常见病毒和木马攻防、Web 攻防、系统漏洞等近千个实例。基本上囊括了用户在平时可能会遇到的黑客问题，使用户能够根据症状快速查找解决办法。同时本书还向用户介绍了如何备份数据以及给自己的重要文件加密，并且对相应的多款加密和数据备份软件做了详尽的介绍，用户可以按照自己的需求选择合适的软件，使自己的电脑更加安全可靠。

☛ 内容新颖

本书在攻防实例的选取上，尽可能实用、新颖、有代表性，这样用户的针对性就会显得更强。同时，对于各种防火墙软件、加密软件和数据备份软件的介绍，也是选用口碑最好，便于操作和下载的软件，这样用户在

使用该软件对自己电脑进行维护就更加方便了。

☞ 语言通俗易懂

本书的文字叙述力求简洁明了，通俗易懂，操作步骤详细明了，条理清楚，思路清晰，使读者无师自通。

全书共分为 8 章，第 1 章主要介绍了黑客常用的攻击方式和防火墙软件的使用；第 2 章至第 6 章主要分类介绍了聊天工具、电子邮件、Web、蠕虫病毒和木马的攻防实例；第 7 章主要介绍了各种操作系统存在的漏洞和解决办法；第 8 章介绍了电脑数据备份、加密等各种保护知识与技巧。

由于编者水平有限，又加上时间仓促，错误与不足之处在所难免，如读者在阅读过程中有什么意见或建议，敬请批评指正。

电脑红宝书编委会

2008 年 8 月

目 录

第1章 黑客来了

1.1 走近黑客.....1	端口扫描攻击.....8
初识黑客.....1	1.3 用户防御.....8
黑客危害.....2	提高安全意识.....8
1.2 黑客的“矛”.....3	采用防火墙机制.....9
口令入侵.....3	隐藏自己的IP地址.....9
放置木马程序.....4	数据备份.....10
Web的欺骗技术.....5	1.4 最强的“盾”.....10
电子邮件攻击.....5	卡帕斯基.....10
“肉鸡”攻击.....6	诺顿.....14
网络监听.....7	ZoneAlarm.....18
利用黑客软件攻击.....7	天网防火墙 (Skynet).....19
安全漏洞攻击.....7	金山网镖.....22

第2章 聊天工具攻防

2.1 MSN 攻防.....24	“OICQthief” 攻防.....33
“Henpeck” 蠕虫攻防.....24	“阿Q 盗密者” v1.1 攻防.....33
“MSN 性感肉鸡” 攻防.....25	“QQSPY” 攻防.....34
“MSN 射手” 攻防.....26	“QQ 号码抢劫者” 攻防.....34
“MSN 骗子” 攻防.....26	“GOP 木马” 攻防.....36
“WORM_FUNNER.A” 病毒攻防.....27	“IPSniper” 攻防.....38
“MSN 小尾巴” 攻防.....28	“蓝色火焰” 攻防.....38
“MSN 飞梭” 攻防.....29	“潜伏猎手” 攻防.....39
“MSN 密码窃贼” 攻防.....29	“QQ 连发器” 攻防.....40
“请客” 病毒攻防.....30	“QQ 杀手” 攻防.....40
“Trojan.Starft” 攻防.....30	“Trojan.PWS” 攻防.....41
2.2 QQ 攻防.....31	“FasleQQ” 攻防.....42
“QQ 尾巴” 攻防.....31	“QQ 之秘密潜入” 攻防.....42
“QQ 神目” 攻防.....32	“爱情森林” 攻防.....42
“QQ 黑暗精灵” 攻防.....32	“QQ 炸弹” 攻防.....43



“狐 Q” 攻防	44	“密码大盗” 攻防	46
“QQ 密码克隆专家” 攻防	44	2.3 Skype 攻防	47
“QQ 千夫指” 攻防	45	“IRCBot 变种” 攻防	47
“QQ 蜗牛” 攻防	45	“Skype 假冒软件” 攻防	48
“KilloICQ” 攻防	45	“MyTob” 攻防	49
“OICQ 密码终结者” 攻防	46	2.4 网络聊天攻防之笔者见	49
“OICQhack” 攻防	46		

第 3 章 电子邮件攻防

3.1 Outlook Express (OE) 及 Outlook 攻防	51	Web 收信漏洞攻防	63
MIME 漏洞攻防	51	“溯雪” 破解免费邮箱密码攻防	64
OutLook 邮件附件漏洞攻防	52	“黑雨” 破解邮箱密码攻防	65
Outlook 收发邮件的漏洞攻防	53	邮件炸弹攻防	65
Outlook 泄露联系人地址的漏洞 攻防	54	垃圾邮件攻防	66
浏览信件硬盘被格式化攻防	54	“Navidad” 攻防	67
“VBS 病毒” 攻防	55	“Worm.Japanize.12288” 攻防	68
“Win32.Harp 病毒” 攻防	57	“班沃母 (Worm.Banwarum.a)” 攻防	69
“WORM_SHOHO.A” 攻防	57	“房产资料” 攻防	69
“Class.CN” 攻防	57	“欢乐时光” 攻防	70
“W97M_melissa” 攻防	58	“新欢乐时光” 病毒 “VBS.KJ” 攻防	73
“Worm.ExplorerZip” 攻防	59	“求职信”	74
“MOYTOB.MX” 攻防	60	“中文求职信” 攻防	75
3.2 Foxmail 攻防	61	“炭疽” 攻防	76
Foxmail 账户查看漏洞攻防	61	3.4 邮件病毒攻防总述	76
Foxmail Punylib.dll 漏洞攻防	62	病毒邮件的入侵形式	76
Foxmail 操作日志漏洞攻防	62	常见的病毒邮件特点	77
Foxmail 泄露联系人漏洞攻防	63	防范和处理病毒邮件	77
3.3 其他邮件攻防	63	电子邮件的安全防范措施	78

第 4 章 Web 攻防

4.1 ASP 脚本攻击	79	验证被绕过攻防	80
用户名和密码破解攻防	79	.inc 文件泄露攻防	80



自动备份被下载攻防.....80	DCP Portal 系统漏洞攻防.....83
特殊字符攻防.....81	Discuz 论坛漏洞攻防.....83
数据库下载漏洞攻防.....81	惊云下载系统 SQL 漏洞攻防.....83
4.2 My Article 文章系统漏洞	动网文章管理系统漏洞攻防.....84
攻防.....82	跨站 Script 攻防.....84
后台管理口令漏洞攻防.....82	Leadbbs 脚本攻防.....85
SQL 注入攻防.....82	JAVA 炸弹攻防.....86
4.3 其他 Web 攻防82	个人空间攻防.....86
BBS XP 论坛账号攻防.....82	4.4 Web 攻防综述86
第 5 章 蠕虫病毒攻防	
5.1 病毒综述88	“雪门”攻防.....113
认清病毒.....88	“阿芙伦”攻防.....113
病毒攻击.....89	“Worm.SirCam”攻防.....115
预防病毒.....90	“Worm.Klez”攻防.....116
5.2 病毒攻防91	“美丽杀手”攻防.....118
宏病毒攻防.....91	“怕怕”攻防.....119
VBS 蠕虫生成器攻防.....92	“辛迪加”攻防.....119
“红色代码”攻防.....94	“Happy99”攻防.....119
“红色结束符 II”攻防.....95	“MALDAL.D”攻防.....120
“红色代码 III”攻防.....97	“Sharpei/Win32.Harp”攻防.....121
“红色代码变种”攻防.....99	“伪装者”攻防.....122
“冲击波”攻防.....100	“网络垃圾 (IV 病毒)”攻防.....123
“冲击波杀手”攻防.....100	“超级密码杀手 007 变种”攻防.....124
“十四日”攻防.....101	“wininit.ini”攻防.....125
“蠕虫王”攻防.....102	“Macro.MakeLove”攻防.....125
“妖怪变种”攻防.....103	“Funlove”攻防.....125
“四维”攻防.....103	“叛逃者”攻防.....126
“大无极”攻防.....105	“汉城”攻防.....127
“大无极变种”攻防.....105	“MSSQL”蠕虫攻防.....128
“小邮差变种 C”攻防.....106	“中国黑客”攻防.....129
“老板公司变种 F”攻防.....107	“超级格式化”攻防.....129
“神速木马”攻防.....109	MP3 文件病毒攻防.....130
“费氏”攻防.....110	“Worm Liac.A”攻防.....130
“爱情后门”攻防.....111	“W32.Perrun”攻防.....131



88 “IRC” 蠕虫攻防.....	131
88 “X-WAY” 攻防.....	132
88 “振荡波” 攻防.....	132
48 “尼姆达” 攻防.....	132

08 “蓝色代码 (CodeBlue)” 攻防.....	133
18 “CIH 病毒” 攻防.....	133
18 “2003 蠕虫王” 攻防.....	134

第6章 木马攻防

6.1 概述木马.....	135
木马的由来.....	135
木马的特征.....	135
木马的危害.....	136
6.2 细述木马.....	137
木马的控制.....	137
木马隐藏.....	139
木马破解.....	141
6.3 常见木马攻防.....	144
“BO2000” 攻防.....	144
“冰河” 攻防.....	152
“广外幽灵” 攻防.....	154
“黑暗天使” 攻防.....	156
“聪明基因” 攻防.....	159
“屏幕幽灵” 攻防.....	159
“Liquid 木马” 攻防.....	160
“QDe1234” 攻防.....	160
“WNC” 攻防.....	161
“风雪” 攻防.....	161
“失恋” 攻防.....	162
“广外女生” 攻防.....	163
“网络神偷” 攻防.....	163
“SubSeven” 攻防.....	164
“灰鸽子” 攻防.....	164
“网络精灵” 攻防.....	165
“WinShell” 攻防.....	166
“无赖小子” 攻防.....	167
“网络魔鬼” 攻防.....	167
“Torjan.Zasil” 攻防.....	168

“PWSteaL.Kaylo” 攻防.....	168
“Trojan.Prova” 攻防.....	169
“网络公牛” 攻防.....	170
“蓝色火焰” 攻防.....	170
“Backdoor.Ducktoy” 攻防.....	171
“BachDoor-ACH” 攻防.....	171
“国际密码” 攻防.....	172
“黑洞 2001” 攻防.....	172
“Funny Flash” 攻防.....	173
“Webber” 攻防.....	173
“Win2000 密码大盗” 攻防.....	173
“短文” 攻防.....	174
“后门” 攻防.....	174
“聪明基因” 攻防.....	175
6.4 手工除马.....	176
清除 “冰河” v1.1 & v2.2.....	176
清除 Acid Battery v1.0.....	177
清除 Acid Shiver v1.0 +.....	177
1.0Mod + lmacid.....	177
清除 Ambush.....	178
清除 AOL Trojan.....	178
清除 Asylum v0.1, 0.1.1~0.1.3 +.....	178
Mini 1.0, 1.1.....	178
清除 AttackFTP.....	179
清除 Back Construction 1.0~2.5.....	179
清除 BackDoor v2.00~v2.03.....	179
清除 BF Evolution v5.3.12.....	179
清除 BioNet v0.84~0.92 + 2.21.....	180
清除 Bla v1.0~5.03.....	180



清除 BladeRunner.....	180	清除 Intruder.....	190
清除 Bobo v1.0~2.0.....	180	清除 IRC3.....	191
清除 BrainSpy vBeta.....	181	清除 Kaos v1.1~1.3.....	191
清除 Cain and Abel v1.50~1.51.....	181	清除 Khe Sanh v2.0.....	191
清除 Canasson.....	181	清除 Kuang logger.....	191
清除 Chupachbra.....	181	清除 Kuang Original v~v 0.34.....	191
清除 Coma v1.09.....	182	清除 Logger.....	192
清除 Control.....	182	清除 Magic Horse.....	192
清除 Dark Shadow.....	182	清除 Masters Paradise.....	192
清除 DeepThroat v1.0~3.1 + Mod (Foreplay).....	182	清除 Matrix v1.0~2.0.....	193
清除 Delta Source v0.5~0.7.....	183	清除 MBK.....	193
清除 Der Spaecher v3.....	183	清除 Millenium v1.0~2.0.....	193
清除 Doly v1.1~v1.7 (SE).....	183	清除 Mine.....	193
清除 Donald Dick v1.52~1.55.....	185	清除 MoSucker.....	194
清除 Drat v1.0~3.0b.....	185	清除 Naebi v2.12~2.40.....	194
清除 Eclipse 2000.....	185	清除 NetController v1.08.....	194
清除 Eclypse v1.0.....	185	清除 NetSphere v1.0~1.31337.....	194
清除 Executer v1.....	186	清除 NetSpy v1.0~2.0.....	195
清除 FakeFTP beta.....	186	清除 NetTrojan v1.0.....	195
清除 Forced Entry.....	186	清除 Nirvana / VisualKiller v1.94 ~1.95.....	196
清除 GateCrasher v1.0~1.2.....	186	清除 Phaze Zero v1.0b + 1.1.....	196
清除 Girlfriend v1.3x (Including Patch 1 and 2).....	187	清除 Prayer v1.2~1.5.....	196
清除 Golden Retreiver v1.1b.....	187	清除 PRIORITY (Beta).....	196
清除 Hack Tack 1.0~2000.....	187	清除 Progenic Password Thief / Keylogger v1.0.....	197
清除 Hack99 Key Logger.....	188	清除 Progenic v1.0~3.0.....	197
清除 Host Control v1.0.....	188	清除 Prosiak beta~0.70 b5.....	197
清除 Hvl Rat v5.30.....	188	清除 Retrieve v1.3.....	197
清除 Iethief.....	189	清除 Revenger v1.0~1.5.....	197
清除 ik97 v1.2.....	189	清除 Ripper.....	198
清除 InCommand v1.0~1.5.....	189	清除 Satans Back Door v1.0.....	198
清除 IndocTrination v0.1~v0.11.....	189	清除 Schwindler v1.82.....	198
清除 inet v2.0~2.0n.....	190	清除 Setup Trojan (Sshare)+Mod Small Share.....	198
清除 Infector v1.0~1.42.....	190	清除 ShadowPhyre v2.12.38~2.X.....	198
清除 iniKiller v1.2~3.2 Pro.....	190		



清除 Share All.....	199
清除 ShareQQ.....	199
清除 Snid v1~2.....	199
清除 Softwarst.....	199
清除 ShitHeap.....	200
清除 Spirit 2000 Beta~v1.2 (fixed).....	200
清除 Stealth v2.0~2.16.....	201
清除 SubSeven~Introduction.....	201
清除 Telecommando 1.54.....	203
清除 The Unexplained.....	203
清除 Thing v1.00~1.60.....	203
清除 Transmission Scout v1.1 ~1.2.....	204

清除 Trinoo.....	204
清除 Trojan Cow v1.0.....	204
清除 TryIt.....	205
清除 Vampire v1.0~1.2.....	205
清除 WarTrojan v1.02.0.....	205
清除 Crat v1.2b.....	205
清除 WebEx (v1.2, 1.3 and 1.4).....	205
清除 WinCrash v2.....	206
清除 WinCrash.....	206
清除 Xanadu v1.1.....	206
清除 Xplorer v1.20.....	206
清除 Xtcp v2.0~2.1.....	207
清除 YAT.....	207

第7章 系统漏洞

7.1 操作系统漏洞及防范.....	208
Windows XP UPNP 漏洞及防范.....	208
Windows XP 账号锁定漏洞及 防范.....	210
Windows XP 远程桌面漏洞及 防范.....	211
Windows XP GDI 拒绝服务漏洞 及防范.....	211
Windows XP 激活特性漏洞及 防范.....	211
Windows XP 的“文件和设置转移 向导”漏洞.....	212
Windows 2000 登录输入法漏洞及 防范.....	213
Windows 2000 NetBIOS 的信息 泄露漏洞及防范.....	215
Windows 2000 系统崩溃漏洞及 防范.....	216
Windows 2000 IIS 服务泄露文件	

内容漏洞及防范.....	217
Windows 2000 MS SQL Server 的 SA 空密码漏洞及防范.....	217
Windows 2000 Telnet 权限提升 漏洞及防范.....	218
Windows2000 Telnet 长用户名拒绝 服务漏洞及防范.....	218
Windows 2000 Telnet 服务拒绝 服务漏洞及防范.....	218
Windows 2000 Telnet 多会话拒绝 服务漏洞及防范.....	219
Windows2000 Telnet 系统调用拒绝 服务漏洞及防范.....	219
Windows2000 Telnet 会话超时导致 拒绝服务及防范.....	219
Windows 2000 Telnet 异域用户 账号的访问漏洞及防范.....	219
Lightwave ConSQLe Server 3200 信息泄露及防范.....	220

Windows ICMP 漏洞及防范.....220	漏洞及防范.....228
Windows NT 登录漏洞及防范.....221	Windows NT 远程访问 Registry
Windows 网络域间信任关系提升	的漏洞及防范.....228
权限漏洞及防范.....223	Windows NT NTFS 的安全设置
Windows NT 安全账户管理数据库	漏洞及防范.....229
被用户复制的防范.....223	Windows NT 文件句柄漏洞及
Windows NT 紧急修复盘更新的	防范.....229
SAM 漏洞及防范.....224	Windows NT 缺省权限设置的漏洞
Windows NT SAM 的系统特权	及防范.....229
人员漏洞及防范.....224	Windows NT 打印操作员组成员
Windows NT SAM 数据库和其他	权限漏洞及防范.....229
服务器文件漏洞及防范.....224	Windows NT FTP 服务漏洞及
Windows NT 远程获得管理员特权	防范.....230
的漏洞及防范.....225	Windows NT 文件移动或者复制
Windows NT 本地获取管理员特权	的漏洞及防范.....230
的漏洞及防范.....225	Windows NT 文件安全权限的漏洞
Windows NT 缺省 Guest 账户漏洞	及防范.....230
及防范.....225	Windows NT NTFS “读取”漏洞及
Windows NT 程序漏洞及防范.....226	防范.....230
Windows NT 用户接管理系统的	Windows NT “删除”权限漏洞及
共享资源的漏洞及防范.....226	防范.....231
Windows NT 无限制地尝试连接	Windows NT 缺省组的权利的删除
系统的漏洞及防范.....226	漏洞及防范.....231
Windows NT 注册失败的次数	Windows NT 进程定期处理机制
无限制的漏洞及防范.....226	“Bug”漏洞及防范.....231
Windows NT 注册失败的次数限制	Windows NT Guest 组成员资格
后解锁的漏洞及防范.....227	漏洞及防范.....231
Windows NT 显示最近一次注册	Windows NT GUI 组最大数目漏洞
用户名漏洞及防范.....227	及防范.....232
Windows NT 保存口令的漏洞及	Windows NT Security Log 的设置
防范.....227	漏洞及防范.....232
Windows NT 口令被不同平台同步	Windows NT 审计文件不完全的
修改的漏洞及防范.....227	漏洞及防范.....232
Windows NT 远程登录漏洞及	Windows NT Secursty Log 集成
防范.....228	漏洞及防范.....232
Windows NT Registry 权限设置	Windows NT 屏幕保护程序 “Bug”



855 漏洞及防范.....233	055 防范.....242
Windows NT 远程查询漏洞及	ACCESS mdb 数据库被下载的
855 防范.....233	漏洞及防范.....242
Windows NT 扫描漏洞及防范.....233	Code.asp 文件会泄露 ASP 代码
Windows NT 端口漏洞及防范.....233	漏洞及防范.....243
Windows NT ping 命令漏洞及	File system object 组件漏洞及
855 防范.....234	防范.....243
Windows NT 空白口令漏洞及	HTML 语句或者 JavaScript 语句
855 防范.....234	的漏洞及防范.....243
Windows NT out-of-band 数据漏洞	ASP 程序密码验证漏洞及防范.....244
855 及防范.....234	WS_FTP Server 2.0.3 漏洞及防范.....244
Windows NT IE 身份验证漏洞及	IPC 漏洞及防范.....244
055 防范.....234	PHP MyAdmin 漏洞及防范.....245
Windows NT HTML 超链接漏洞	PHP BB 远程 SQL 查询处理漏洞
855 及防范.....235	及防范.....245
7.2 浏览器漏洞及防范.....235	PHP BB \$1_statsblock 变量远程
IE6.0 泄露信息的漏洞及防范.....235	执行代码漏洞及防范.....246
IE5.0 访问 FTP 站点时的漏洞及	PH Projekt 漏洞及防范.....246
055 防范.....236	BSDi 4.2 漏洞及防范.....246
IE5.0 ActiveX 漏洞及防范.....236	PHP-Nuke 插入 SQL 语句漏洞及
7.3 服务器漏洞及防范.....237	855 防范.....247
Microsoft SQL Server 漏洞及防范.....237	PHP-Nuke 文件泄露和上传漏洞及
C Runtime 函数库内格式字符串	855 防范.....247
漏洞及防范.....237	PHP-Nuke 的 Network Tool 漏洞及
SQL Server 2000 “扩展存储过程”	855 防范.....247
漏洞及防范.....238	PHP-Nuke 的 Cookie 漏洞及防范.....247
ASP 泄露源程序漏洞及防范.....238	PHP-Nuke 跨站脚本执行漏洞及
IIS 泄露 ASP 源程序漏洞及防范.....239	防范.....248
Null.htw IIS 漏洞及防范.....239	PHP-Nuke 附件漏洞及防范.....248
HTR 文件漏洞及防范.....239	Unix Manual 漏洞及防范.....248
IIS 远程拒绝服务漏洞及防范.....241	PHP File Exchange 漏洞及防范.....249
IIS HACK 漏洞及防范.....241	Perl 用户输入漏洞及防范.....249
Codebrws.asp 和 Showcode.asp	Perl Exec() 函数漏洞及防范.....250
漏洞及防范.....241	Perl System() 函数漏洞及防范.....250
MDAC 执行本地命令漏洞及防范.....242	Perl 单引号漏洞及防范.....251
ISAPI 缓冲区扩展溢出漏洞及	Perl Eval() 漏洞及防范.....251

Perl Setuid 脚本漏洞及防范	251	禁用内容选项	275
Perl 缓存区溢出漏洞及防范	251	禁止更改分级设置	276
7.4 系统安全配置	252	禁止更改证书设置	276
Windows XP 的安全配置	252	禁用表单的自动完成功能	276
Windows 2000 的安全配置	258	禁用自动完成保存密码	277
Windows NT 的安全配置	262	禁止更改高级页设置	277
7.5 注册表防护	264	禁用连接选项	277
注册表基本操作	264	对拨号连接实行“自动检测”	278
防止其他人非法编辑注册表	266	禁用缓存自动代理脚本	278
隐藏局域网上的服务器	267	取消资源管理器的文件菜单	278
不允许用户拨号访问服务器	267	禁用 Internet 连接向导	279
隐藏“控制面板”	267	禁止更改代理服务设置	279
隐藏用户登录名	268	显示有关代理脚本下载失败的	
禁止其他人对桌面进行任意设置	268	出错信息	279
抵御 BackDoor 的破坏	268	禁用程序选项	280
禁止通过“文件夹选项”显示隐藏		禁止更改默认浏览器检查	280
文件	269	禁止更改日历和联系人的设置	280
屏蔽对软盘的网络访问功能	269	禁止更改邮件设置	281
隐藏“网上邻居”图标	270	禁用“重置 Web 设置”功能	281
限制用户使用指定程序	270	禁用高级选项	281
不允许他人设置屏幕保护密码	270	设置密码的安全要求	282
防范非法入侵 Windows XP 系统	271	Windows XP 安全日志管理技术	282
隐藏硬盘中的分区	271	禁止“显示”属性对话框中的	
将文件系统设置为 NTFS 格式	271	“Web”页	283
抵御 WinNuke 黑客程序对计算机		隐藏任务栏上按右键时弹出的	
的攻击	272	菜单	283
禁止用户锁定计算机	272	禁用注册表编辑器 Regedit	283
禁止查看指定磁盘驱动器的内容	272	禁止修改计算机账户密码	284
禁止运行命令解释器和批处理		使用注册表解锁“光盘保镖”	284
文件	273	恢复对注册表的错误修改	285
禁止用户更改口令	273	7.6 局网络隐患及安全设置	285
禁止更改主页设置	274	蓝屏死机解决	286
禁止更改辅助功能设置	274	密码漏洞解决	286
禁止更改临时文件设置	274	个人隐私泄露问题解决	286
禁止更改历史记录设置	275	木马入侵隐患解决	287
禁用安全选项	275	安全设置共享文件	287



安全设置共享打印机.....	288
屏蔽网络设置.....	289
7.7 SQL Server 2000 的安全	
配置.....	290
系统设置.....	290
密码安全设置.....	291

账号安全设置.....	291
数据库日志安全设置.....	291
协议加密.....	292
扩展存储过程.....	292
网络连接的 IP 限制.....	292
TCP/IP 端口安全设置.....	292

第 8 章 密码攻防及数据防护

8.1 密码攻防	294
Windows 2000/XP 登录密码.....	295
Windows Me 登录密码.....	297
Windows 98 登录密码.....	297
LINUX 登录密码.....	298
Windows 屏幕保护程序密码.....	298
Winzip 密码.....	298
Winrar 密码.....	299
Office 系列密码.....	300
Arj 密码.....	300
CMOS 密码.....	301
Internet 选项里面的“分级审查” 密码.....	302
利用文件属性加密.....	304
利用回收站加密.....	305
利用 NTFS 文件系统加密.....	305
QQ 密码.....	306
网络游戏密码.....	307
Foxmail 和 Outlook Express 密码.....	309
8.2 加密工具简介	310
EasyCode.....	311
Encrypted Magic Folders.....	312
DigiSecret.....	313
PrivateEXE.....	315
Private Pictures.....	316

WinXfiles.....	317
Z-File.....	318
Invisible Secrets.....	319
Hide In Picture.....	320
文件密使.....	320
Password Door.....	321
我的保险箱.....	322
8.3 数据备份	323
Ghost 工具备份及恢复.....	324
操作系统自带的备份工具.....	335
瑞星备份工具.....	337
一键还原精灵.....	338
Image It.....	339
8.4 硬盘的正确维护和使用	341
硬盘检测手段.....	342
硬盘防护手段.....	349
硬盘故障排除.....	350
8.5 硬盘空间管理	355
系统垃圾文件.....	355
磁盘清理.....	356
磁盘整理工具.....	359
磁盘空间管理.....	361
磁盘配额管理.....	362
远程存储管理.....	365

第1章 黑客来了

从古至今，人们对叛逆者的角色有着太多的偏爱。就像梁山好汉，劫富济贫，替天行道，是人们心目中的英雄。今天的 Internet 越来越普及，越来越多的人已经离不开网络。古代悲歌慷慨的豪侠气概，后世迄未泯灭。作为网络世界另一极的游侠，现在是出场的时候了。他们为了用户能够更加自由地使用网络，作了很多贡献。

但是，每个世界都是有坏蛋存在的。古有“李鬼”，在 Internet 商业化的今天，出现了越来越多的淘金者，也出现了“打家劫舍”的“李鬼”，他们的名字叫“黑客”。

可惜，很多人对黑客的态度却很暧昧，毕竟开始时，黑客的目标不是普通的用户，而是一些防守森严的“太空堡垒”，不少人是都抱着看热闹的态度，更有甚者认为黑客是天才，是在网络世界飞檐走壁的独行侠，是心目中的英雄。

记得一个朋友说过这样的话：“一个没有英雄的时代是可悲的，一个把恶棍奉为英雄的时代则是可耻的。”随着黑客技术的平民化，黑客工具的泛滥，黑客的门槛越来越低，越来越多的普通用户遭到攻击，电脑安全已经成为一张薄纸，这时候，大家才如梦初醒，惊呼：“黑客来了！”

1.1 走近黑客

初识黑客

“黑客”(Hacker)源于英语动词 hack，意为“劈砍”，引伸为干一件非常漂亮的工作。要给“黑客”下一个准确的定义是非常困难的，因为在其发展的历史中，它自身一直在进行着微妙的演变。

一般认为，黑客起源于 20 世纪 50 年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。20 世纪 60 年代，“黑客”指独立思考、奉公守法的计算机迷。他们利用分时技术允许多个用户同时执行多道程序，