



新手入门

黑客

鹰派联盟权威推荐
中国第一黑客团队

7种武器攻防 108招

工欲善其事 必先利其器

【工具·实战篇】

仲治国 编著

挑战黑客

孔雀翎
扫描与嗅探

碧玉刀
进程与端口安全

离别钩
安全检测与黑客兵器

长生剑
木马与远程控制

霸王枪
流氓软件与病毒查杀

拳头
帐户管理与加密解密

多情环
网络盗号与安全防范

超值光盘

价值88元正版软件大礼包
华夏黑客同盟视频教程
防病毒反黑工具
病毒库升级包
网络扫描工具
密码解除工具



7种武器攻防 108招

【工具·实战篇】

仲治国 编著

内 容 提 要

《黑客7种武器攻防108招》是一本专门为广大电脑爱好者准备的黑客入门类图书。全书借鉴了古龙《七种武器》的模式，结合当前最流行的黑客攻防工具，进行了具体详细的讲解，读者可以按部就班，迅速识破黑客攻防伎俩并进行有效防范。

全书内容共包含七大板块，分别是：碧玉刀——进程与端口安全、孔雀翎——扫描与嗅探实例、拳头——账户管理与加密解密、多情环——网络盗号与安全防范、长生剑——木马与远程控制、霸王枪——流氓软件与病毒查杀、离别钩——安全检测与黑客兵器。各大板块既独立成章，又相互关联，涉及到黑客攻防的方方面面，构建起完美的黑客攻防体系。

本书采用全程图解的形式，即便是入门的读者也能快速学会黑客攻防知识，从而采取最有效的方式捍卫网络安全。

多媒体教学光盘运行说明

运行环境：Windows 98/Me/2000/XP/2003；

操作说明：光盘放入光驱后会自动运行，也可以打开光盘目录，运行hacker.exe文件即可；

光盘内容：图书配套软件以及精彩黑客攻防视频教学（参见“多媒体光盘内容简介”页）。

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负！

书 名：黑客7种武器攻防108招
编 著：仲治国
执行编辑：李 勇 何 磊
封面设计：程 佳
责任编辑：李 萍
监 制：吕美亮
出版单位：山东电子音像出版社
地 址：济南市胜利大街39号
邮 政 编 码：250001
电 话：(0531)82098390
发 行：山东电子音像出版社
经 销：各地新华书店、报刊亭
C D 生产：北京中联光碟有限公司
文 本 印 刷：重庆联谊印务有限公司
开 本 规 格：787mm × 1092mm 1/16 16 印张 250 千字
版 本 号：ISBN 978-7-89481-004-5
版 次：2007年7月第1版 2007年7月第1次印刷
定 价：28.00元(1CD+配套书)



计谋迭出，胸藏攻防先见之明

网络就是战场，安全就是用兵。

战场上硝烟弥漫，鲜血迸溅；网络中黑客针锋相对，明争暗斗！

黑客世界的刀光剑影总让人感到神秘莫测。

正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

“黑客道”丛书自2005年推出以来，得到了很多读者的喜爱和好评，多次荣登全国图书畅销排行榜，图书历经多次加印，累计销售达20万册，创下黑客类图书的多个NO.1：

第一套兵法战术与电脑安全相结合的黑客类图书

第一套讲故事与授谋略相结合的黑客图书

第一套将古代兵法完美演绎的黑客实战宝典

.....

应读者的要求，再版的“黑客道”丛书进行了全新修订：增加了最新出现的各种黑客技术和黑客工具的应用内容，新版“黑客道”将给大家带来更加实用的黑客技巧与安全方案，让你完全了解网络安全之道，有效防范黑客攻击。

一名技艺高超的黑客无非体现在以下两方面：其一是娴熟的黑客工具应用，其二是独到的谋略技巧施展。“黑客道”丛书正是从以上两个方面的黑客攻防必备技能展开。丛书内容设置为：

《黑客攻防36计》(谋略●技巧篇)：以我国最负盛名的神奇兵书《三十六计》为蓝本，从三十六个方面详尽地进行了实战式的黑客入侵与防御演练，将古代兵法韬略在黑客攻击防范中体现得淋漓尽致！

《黑客7种武器攻防108招》(工具●实战篇)：源自武侠巨匠古龙大师的扛鼎之作《七种武器》，并结合当前黑客最流行的一百零八种工具进行了详细的讲解。

黑客其实就这么几招，有效防范黑客入侵也并非只是专家的绝活，是要你有兴趣和决心，你一样能行！

最后，衷心地祝愿广大读者通过本书的阅读快速了解黑客知识：掌握黑客绝技高招，轻松捍卫网络安全！

编者

2007年7月

多媒体光盘内容简介



● 防毒反黑工具

本栏目收录了多款安全防范工具，能抵御黑客入侵，消除流氓软件困扰。

● 病毒库升级包

本栏目收录了常用杀毒软件升级包，即使在脱机的环境中也能更新病毒库。

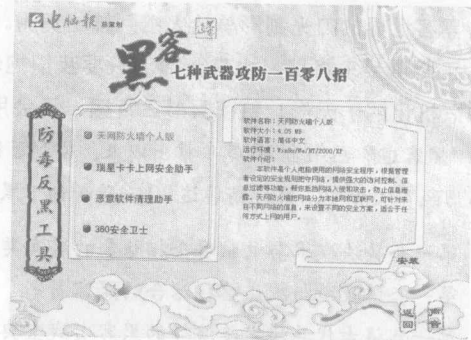
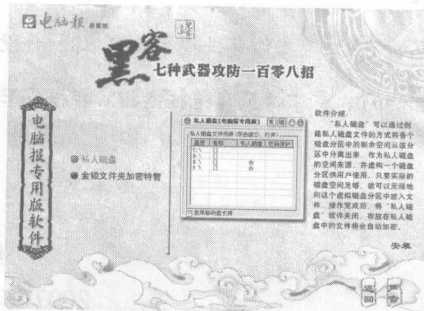
● 黑客攻防视频教程

(华夏黑客同盟网站授权)

- ※ IDS & 蜜罐系统的实现
- ※ “黑客迷你QQ”使用方法
- ※ 服务器安全配置
- ※ 禁止服务删除共享
- ※ 巧妙管理系统进程
- ※ Ping 的正确使用
- ※ SysShield 使用教学
- ※ 安装 Radmin 服务端
- ※ 局域网中实现二级代理
- ※ 保护 Office 2003 文档
- ※ 远程网络维护系统
- ※ 轻松搞定文件关联

● 电脑报专用版软件

本栏目赠送的是电脑报专用版软件：“私人磁盘”、“金锁文件夹加密特警”，它们能更好地加密计算机数据资料，保护隐私信息。



● 网络扫描工具

本栏目收录的工具能扫描网络计算机端口及 IP 地址，有助于用户分析漏洞。



● 密码解除工具

如果你因忘记密码无法打开文档的话，不妨试试本栏目提供的密码解除工具。

目录

第一篇

碧玉刀——进程与端口安全

第1招 通透认识系统进程	2
一、明明白白系统进程	2
二、关闭进程和重建进程	2
三、查看进程的发起程序	3
四、查看隐藏进程和远程进程	4
五、杀死病毒进程	5
第2招 巧妙识别真假 SVCHOST.EXE 进程	6
一、认识 SVCHOST.EXE 进程	6
二、识别 SVCHOST.EXE 进程的真伪	6
第3招 当心 Explorer、iexplore 两进程	7
一、认识 Explorer.exe 进程	7
二、Explorer.exe 容易被冒充	7
三、当心 iexplore.exe 进程	9
第4招 Windows 进程管理器	10
一、系统进程管理	10
二、恶意进程分析	10
第5招 超级巡警保护系统进程	11
一、超级巡警查杀木马	11
二、超级巡警实时防护系统	11
三、超级巡警的帐号保险箱	12
四、系统安全增强工具	12
五、妙用 SSDT 工具清除流氓软件	13
第6招 巧设端口防木马	14
一、什么是计算机端口	14
二、端口的分类	14
三、开启和关闭端口	14
四、图形化的端口查看工具	15
第7招 看好远程终端服务 3389 端口	16
一、重定向本机默认端口	16
二、3389 端口“门”前是非多	17
三、3389 端口入侵与防范	18

目录

第二篇

第8招 端口扫描保平安	19
一、常见端口剖析	19
二、端口扫描利剑出鞘	20
第9招 火眼金睛识木马——Port Reporter	22
一、安装和卸载 Port Reporter	22
二、配置 Port Reporter “捉” 木马	23
三、日志文件分析	24
四、根据端口查杀木马	24

孔雀翎——扫描与嗅探实例

第10招 安全检测网上行	26
一、赛门铁克在线检测	27
二、天网在线安全检测	28
三、PC Flank 安全检测	29
第11招 扫描的追踪与防范	29
一、什么是扫描	29
二、扫描实战	30
三、扫描的反击与追踪	33
四、让系统对 Ping 说 “NO”	34
第12招 网页安全扫描器	36
一、漏洞扫描	36
二、查看安全漏洞	37
第13招 X-scan 查本机隐患	38
一、用 X-scan 查看本机 IP 地址	38
二、添加 IP 地址	39
三、开始扫描	39
四、X-SCan 高级设置	39
第14招 LANNSS 扫描局域网安全隐患	42
一、扫描局域网内计算机的安全漏洞	42
二、查看扫描到的漏洞	44
第15招 RPC 漏洞扫描器	44
一、RPC 漏洞带来的危险	44
二、RPC 漏洞分析	44

目录

第二篇

三、扫描RPC漏洞	45
第16招 WebDAVScan 漏洞扫描器	46
一、WebDAV 漏洞解析	46
二、扫描WebDAV 漏洞	46
三、WebDAV 漏洞防治方法	46
第17招 SQL 安全扫描器 Hscan	47
一、SQL 漏洞危险的由来	47
二、黑客入侵解析	47
第18招 玩转NC 监控与扫描功能	48
一、监听本地计算机端口数据	48
二、监听远程计算机端口信息	49
三、将NC 作为扫描器使用	49
第19招 实时监控本地电脑使用情况	50
一、添加使用密码	50
二、设置弹出热键	50
三、监控浏览过的网站	51
四、键盘输入内容监控	51
五、程序执行情况监控	52
第20招 使用影音神探嗅探在线视频地址	53
一、配置“影音神探”	53
二、快速捕获视频的下载地址	53
三、实时远程IP 连接	54
第21招 经典嗅探器之 Iris	54
一、Iris 的工作原理	54
二、用 Iris 捕获数据	55
三、防范 Iris 的嗅探	57
第22招 用 NetXray 嗅探器捕获数据	57
一、认识 NetXray	57
二、NetXray 捕获数据	58
三、NetXray 其他功能	59
第23招 用 SpyNet Sniffer 嗅探下载地址	60
一、用 SpyNet Sniffer 播放音乐或视频	60
二、用 SpyNet Sniffer 捕获下载地址	60

目录

第三篇

第24招 用ProtectX 防御扫描器追踪	61
一、ProtectX 实用组件解析	61
二、防御扫描器攻击	62

拳头——帐户管理与加密解密

第25招 办公文档加密与解密	64
一、使用WordKey 恢复Word 密码	64
二、WORD97/2000/XP 密码查看器	65
三、轻松查看Excel 文档密码	65
四、快速查看WPS 密码	66
第26招 压缩文件加密与解密	66
一、RAR Password Cracker	66
二、“多功能密码破解软件”恢复密码	68
第27招 妙招恢复Windows XP 管理员密码	69
一、删除SAM 文件清除管理员密码	69
二、从SAM 文件中查看密码	69
三、修改管理员密码	69
四、用ERD Commander 恢复XP 密码	70
五、未雨绸缪——用好密码重置盘	72
第28招 轻松解除Syskey 双重加密	72
一、Syskey 双重加密方法	72
二、轻松解除Syskey 加密	74
三、Sykey 加密注意事项	74
第29招 体验与众不同的分时段加密	75
一、软件的特色功能	75
二、管理加密用户	75
三、加密文件夹	75
四、设置自解密时间	76
五、激活加密功能	76
第30招 与众不同的图片加密好帮手	76
一、新建一个加密档案	77
二、导入要加密的图片	77
三、解密文件	77

目录

第三篇

第31招 WinRAR“另类”加密方法	78
一、利用MP3巧加密	78
二、让加密文件更安全	78
第32招 我的程序你别动——WinGuard	79
一、设置程序保护密码	79
二、设置要限制的程序	79
三、文件/文件夹加密	80
四、锁定其他选项	80
第33招 文件分割巧加密	81
一、分割文件	81
二、合并文件	81
第34招 生成自解密文件的“机器虫加密”	82
一、加密文件	82
二、解密文件	82
第35招 虚拟磁盘加密	83
一、创建虚拟加密磁盘	83
二、虚拟磁盘的使用	84
第36招 来自微软的顶级密码箱	85
一、创建密码箱	85
二、文件加密与解密	86
三、文件加密异地传输	86
第37招 文件隐藏巧加密	87
一、创建隐藏文件夹	87
二、操纵“隐藏文件夹”	87
三、编辑和删除隐藏文件夹	88
四、文件隐藏大师项设置	88
第38招 为你的U盘加把锁	89
一、加密整个U盘	89
二、部分数据加密	89
三、密码解除	90
第39招 军用级硬盘加密	90
一、创建虚拟磁盘空间	90
二、对数据文件加密	91
三、在虚拟磁盘中创建“虚拟磁盘”	92

目录

第四篇

- 第40招 解除各种网络登录密码 93
- 一、找回“自动完成”密码 93
 - 二、用黑雨密码探测器恢复邮箱密码 93
 - 三、巧用 MessenPass 查看 MSN 密码 94

多情环——网络盗号与安全防范

- 第41招 菜鸟盗Q的利器——QQ大杀器 96
- 一、当心QQ号、Q币、密保被盗 96
 - 二、自动生成QQ尾巴 96
 - 三、文件捆绑、自动弹出网页 97
- 第42招 提防“完美QQ大盗”盗QQ 97
- 一、初识完美QQ大盗 97
 - 二、Q币、QQ邮件、密保一网打尽 98
 - 三、对杀毒软件免疫 98
- 第43招 防范“啊拉QQ大盗”盗取QQ 99
- 一、“邮箱收信”方式盗QQ 99
 - 二、“网站收信”方式盗QQ 100
 - 三、“啊拉QQ大盗”防范方法 100
- 第44招 QQ密码保护的克星——QQ密保大盗 100
- 一、木马客户端制作方法 101
 - 二、轻松盗取QQ密码 101
 - 三、巧妙突破密码保护 101
 - 四、巧用QQ申诉信息“夺取”QQ号 102
- 第45招 当心“QQ掠夺者”盗取QQ 102
- 一、认识QQ掠夺者 103
 - 二、QQ盗取曝光方法 103
 - 三、防范QQ掠夺者 103
- 第46招 防范“QQ破密使者”盗取QQ 104
- 一、本地盗取QQ揭秘 104
 - 二、防范QQ破密使者 104
- 第47招 在线获取QQ揭秘 105
- 一、在线获取介绍 105
 - 二、QQExplorer 在线破解及其防范 105

目录

第四篇

- 第48招 解读“密码使者”截获QQ 106
- 一、初识“密码使者” 106
 - 二、“密码使者”作案剖析 106
 - 三、防范QQ被盗取的应对措施 107
- 第49招 来自“QQ枪手”的攻击 107
- 一、QQ枪手简介 107
 - 二、QQ枪手盗号探秘 107
- 第50招 “QQ机器人”盗号也疯狂 108
- 一、安装运行QQ机器人 108
 - 二、配置QQ机器人 108
- 第51招 防范“OICQ密码轻松盗”监听 109
- 一、曝光盗号方法 109
 - 二、防范OICQ密码轻松盗的监听 110
- 第52招 识破“QQ密码保护”的骗局 110
- 一、认识“QQ密码反保精灵” 110
 - 二、“QQ密码反保精灵”骗术曝光 110
 - 三、防范QQ密码保护的骗术 110
- 第53招 全面武装打造安全QQ 111
- 一、妙用磁盘读写权限彻底封杀QQ广告 111
 - 二、为QQ硬盘设置密码 111
 - 三、为QQ通讯录设置密码 112
 - 四、看好你的Q币 112
- 第54招 用“防盗专家”为QQ保驾护航 113
- 一、认识防盗专家 113
 - 二、自动关闭QQ广告 113
 - 三、取回QQ密码 113
 - 四、QQ内核修改 114
 - 五、QQ病毒查杀 114
 - 六、无敌QQ外挂 114
 - 七、“防盗专家”的其他功能 114
- 第55招 伸向MSN的黑手MSN Messenger Hack 115
- 一、认识MSN Messenger Hack 115
 - 二、MSN盗取揭秘 115
 - 三、防范MSN Messenger Hack 116

目录

第五篇

第56招 MSN 密码查看帮凶 —— MessenPass	116
一、MessenPass 简介	116
二、查看 MSN 密码解析	116
三、防范 MessenPass	116
第57招 防范 E 话通靓号被盗	117
一、解读 E 话通号码被盗	117
二、防范 E 话通靓号被盗	118
第58招 联众密码监听器	118
一、当心“联众密码监听器”	118
二、找回丢失的联众密码	119
第59招 防范“传奇密码邮差”	119
一、传奇密码盗取方式揭秘	119
二、警惕“传奇密码邮差”	119
三、拒绝传奇盗号	120
第60招 揪出内鬼——密码监听器	121
一、“密码监听器”盗号披露	121
二、找出“卧底”拒绝监听	122
 长生剑——木马与远程控制 	
第61招 图片摇身变木马	124
一、图片与程序的“捆绑”	125
二、COPY 命令也玩捆绑	126
第62招 冰河的反入侵实战	126
一、什么是木马的反入侵	126
二、木马入侵与反入侵实战	126
三、反弹式木马的反入侵	130
第63招 DLL 木马追踪防范	130
一、动态嵌入式 DLL 木马介绍	130
二、DLL 木马的清除方法	132
第64招 防范变幻网页木马	134
一、观察进程寻找木马	134
二、如何用杀毒软件进行快速诊断	134
三、木马的下载与运行	134

目录

第五篇

四、MIME 邮件扩充协议简介	135
五、如何清除木马	137
六、网页木马防范方法	137
第 65 招 剖析广外幽灵的隐身	139
一、什么是广外幽灵	139
二、广外幽灵的工作原理	139
三、广外幽灵的清除方法	140
第 66 招 用 WinVNC 体验远程控制	141
一、配置 WinVNC 服务器	141
二、客户端远程连接	141
第 67 招 使用 WinShell 实现远程控制	142
一、WinShell 简介	142
二、配置服务器端	142
第 68 招 灰鸽子远程控制实例	144
一、远程控制的罪魁祸首——灰鸽子	144
二、灰鸽子系统配置	144
三、生成并运行服务端	145
四、发送服务端给被攻击者	146
五、远程控制你的电脑	146
六、手工卸载灰鸽子服务端	147
第 69 招 感受 Serv-U 的远程控制	148
一、服务器配置	148
二、工作站配置	148
第 70 招 探密远程开启视频的木马	149
一、远程开启视频的必要性	149
二、如何开启远程视频	149
三、服务器端的清除	151
第 71 招 用 TFTP 实现上传下载	151
一、安装 TFTP 服务	151
二、使用 TFTP 服务	152
三、防范 TFTP 入侵	153
第 72 招 使用 QuickIP 进行多点控制	153
一、QuickIP 功能介绍	153
二、设置 QuickIP 服务端	154
三、配置 QuickIP 客户端	154

目录

第六篇

四、利用 QuickIP 远程控制	155
第 73 招 巧用屏幕间谍定时抓屏	156
一、屏幕截图	156
二、设置抓取时间间隔	156
第 74 招 实战命令行下的远程控制 PsExec	158
一、进入 Telnet 操作状态	158
二、执行本地程序	158
三、启动远程服务	158
第 75 招 用 URLy Warning 监控远程信息	159
一、URLy Warning 简介	159
二、URLy Warning 远程监控	159
第 76 招 合并可执行程序嵌入木马	160
一、合并 EXE 文件	160
二、修改合并后的 EXE 文件图标	160
第 77 招 远程控制好帮手 PcAnywhere	161
一、PcAnywhere 安装步骤	161
二、PcAnywhere 基本设置	161
三、使用 PcAnywhere 进行远程控制	162
 霸王枪——流氓软件与病毒查杀	
第 78 招 瑞星卡卡清除流氓软件	165
一、认识“流氓软件”及其分类	165
二、瑞星卡卡根除“流氓软件”	165
第 79 招 360 安全卫士查杀恶意软件	168
一、系统漏洞修复	168
二、查杀恶意软件	169
三、全面系统诊断与修复	169
四、免费查杀病毒	170
第 80 招 金山系统清理专家	170
一、恶意软件查杀	171
二、两种方式修复 IE	171
三、进程和启动项管理	172
四、历史痕迹清理	172

目录

第六篇

- 五、其他特色功能介绍 172
- 第81招 Windows 流氓软件清理大师 173
 - 一、恶意软件卸载 173
 - 二、垃圾文件清理及系统优化 173
- 第82招 微软反间谍高手 174
 - 一、初识反间谍软件利器 174
 - 二、手动扫描查杀间谍软件 174
 - 三、设置定时自动扫描 175
 - 四、开启实时监控 176
 - 五、四款特色安全工具 176
- 第83招 Spybot-Search & Destroy 清除间谍 177
 - 一、使用 Spybot 清除间谍软件 177
 - 二、用 Spybot 恢复误删除的文件 178
 - 三、设置 Spybot 对间谍软件免疫 178
 - 四、用 Spybot 查找启动项中的间谍 178
- 第84招 间谍杀手 Ad-aware 179
 - 一、设置软件更新 179
 - 二、使用 Ad-aware 全面扫描系统 179
 - 三、使用 Ad-aware 快速清除任务 180
- 第85招 用 Spy Sweeper 铲除间谍软件 180
 - 一、软件安装与设置 180
 - 二、铲除间谍软件实战 181
- 第86招 清理浏览器中的“流氓软件”插件 181
 - 一、使用 Windows XP SP2 插件管理功能 182
 - 二、IE 插件管理专家 182
- 第87招 防范“流氓软件” 182
 - 一、及时更新补丁程序 182
 - 二、禁用 ActiveX 脚本 183
 - 三、加入受限站点 183
 - 四、修改 HOSTS 文件 183
 - 五、设置网页安全扫描 183
 - 六、修改注册表 184
- 第88招 使用瑞星 2007 杀毒 184
 - 一、全新的虚拟脱壳 185
 - 二、开机“抢先”杀毒 185

目录

第七篇

三、独特的“碎甲”技术击溃 Rootkits.....	185
四、主动漏洞扫描、修补.....	185
五、易用的文件粉碎功能.....	186
六、嵌入式查杀病毒.....	186
第89招 使用卡巴斯基杀毒软件杀毒.....	187
一、基本查杀方法.....	187
二、完全查杀.....	187
三、更新病毒库.....	188
第90招 熊猫钛金版查杀病毒.....	188
一、基本查杀.....	188
二、启用防间谍软件保护.....	189
三、防范未知威胁.....	189
第91招 天网防火墙.....	190
一、天网防火墙初步应用.....	190
二、天网安全设置.....	191
三、检查并修复系统漏洞.....	192
第92招 诺顿网络安全特警.....	193
一、配置安全特警.....	193
二、启用诺顿网络安全特警.....	194
三、程序扫描.....	194
四、隐私控制.....	195
五、在线安全检测.....	195
六、封锁恶意IP.....	196
七、端口安全防范.....	197
第93招 免费的专业防火墙Kerio.....	197
一、Kerio 基本应用.....	197
二、调整Kerio 过滤机制.....	198

离别钩——安全检测与黑客兵器

第94招 单机版入侵检测系统NID.....	201
一、NID 简介.....	201
二、NID 基本设置.....	201
三、NID 规则设置与使用.....	201