超值学习工具盘　资源与欣赏俱全

POPULAR COMPUTER WEEKLY 2013 SUPPLEMENT

电脑报 2013 增刊

黑客攻防与电脑安全年度应用方案

电脑报 编

黑客攻击与防范

密码 / 破解 / 盗号 / 挂马 / 远程监控 / 无线攻防

黑客攻防实例剖析 / 攻防技巧倾囊相授 / 安全配置轻松上手

16个精彩专题

150套黑客攻防方案 1500幅直观图解

→ 菜鸟黑客篇

密码 / 进程 / 病毒 / 代理服务器
…息 智能手机与微博安全
…解析 移动存储与图片病毒
…李鬼 自己动手揪出“黑线”进程
…衣 IP地址追踪和隐藏

→ 攻防实例篇

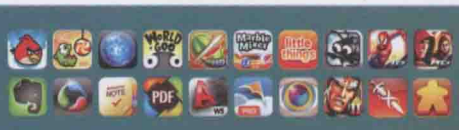
木马 / 嗅探 / 网络钓鱼 / 远程监控 / 无线攻防
决胜千里 轻松进行远程监控
防不胜防 网站挂马与钓鱼
拒绝被“蹭”无线网络破解实例剖析
近水楼台 局域网嗅探与网吧攻防解析

→ 安全防范篇

系统安全 / 数据库 / 服务器 / 入侵检测
网络暴力 拒绝服务和网络炸弹攻防
直击核心 论坛与数据库攻防实战
千防万护 服务器入侵与防范解析
杜绝隐患 入侵检测与日志管理

超值学习工具盘 资源与欣赏俱全
24款电脑安全必备工具
账号密码保护 / 防火墙 / 杀毒软件/木马查杀
进程管理 / 赠精彩黑客攻防视频、电子书

超值赠送 金山毒霸



电脑报增刊

2013 ZENGKAN

黑客攻防与电脑安全年度应用方案

电脑报 编

电脑报电子音像出版社
CPCW ELECTRONIC & AUDIOVISUAL PRESS

内容提要

《电脑报2013增刊——黑客攻防与电脑安全年度应用方案》关注最新黑客攻防技术，荟萃16大精彩专题，包含150套黑客攻防方案，累计1000余条操作技巧。具体内容包括：密码安全、网络盗号、移动存储安全、图片病毒、IP地址追踪和隐藏、局域网嗅探与网吧攻防、网站挂马与钓鱼、无线网络破解实例、拒绝服务和网络炸弹攻防，以及系统账户与口令攻防、论坛与数据库攻防、服务器入侵与防范、入侵检测与日志管理等，让大家洞悉黑客攻防招式，轻松捍卫网络安全！

《电脑报2013增刊——黑客攻防与电脑安全年度应用方案》每一个专题都是经过电脑报编辑精心提炼的热点应用方案：每一个方案都可以从头到尾帮你完成一项完整的应用任务；每一条秘技都会让你有茅塞顿开的感觉。专题方案详尽、实用性强、汇集各种电脑热门应用，适合初、中级电脑用户以及广大的电脑爱好者阅读与收藏。

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！

电脑报2013增刊——黑客攻防与电脑安全年度应用方案

编　　著：电脑报
责任编辑：连　果
版式设计：郑　兰　杨　亚
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
服务电话：(023)63658888-12031
发　　行：重庆电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：四川省蓥山数码科技文化发展有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：787mm×1092mm　1/16　　19印张　　350千字
版　　号：ISBN 978-7-89476-718-9
版　　次：2012年9月第1版　　2012年9月第1次印刷
定　　价：35.00元（1CD+手册）

电脑报增刊 Preface

专注黑客攻防热点 全面解决安全难题

● 电脑报年度大作 11年持续畅销图书 ● 专注热点 只谈应用 精品方案 全面解决

● 荟萃精华：软件/硬件/影音/摄影/平板/导航/网络生活/网上赚钱/黑客安全……

打开《电脑报2013增刊》，走入电脑与数码完全应用空间！

电脑与数码是当今人们生活与科技应用的两大主题，选用电脑、时尚数码、玩转网络、摄影影音、平板手机、防黑安全、品质生活……如果你不想OUT于主流社会的科技潮，如果你想利用科技产品全面提升工作学习效率，提高生活品质，掌握热门的电脑与数码应用方案，精通各种技巧与排困解难方法，这套书就是您必需的！

更专注，更专业，更实用！

作为电脑报的一年一度的重磅大作，《电脑报增刊》从2002年出版以来，就以专门盘点大众关注度较高的IT应用热点、聚焦热门电脑应用方案，赢得广大读者的喜爱与首肯，累计销售数量已经突破280万册，直接和间接读者估计超过600万人。《电脑报增刊》已成为电脑用户进阶必读的经典书目，相当一部分电脑用户甚至将这套书作为年度标志性读本珍藏。

特色鲜明，非看不可！

1.独立专题，紧扣热点：《电脑报2013增刊》的所有热点内容一律采用专题式、模块化的形式组织，有助于读者按需阅读。

2.解决方案，精巧实用：《电脑报2013增刊》纯粹以“应用方案”为出发点的编写理念，充分体现了“实用至上”的编辑思想。全套三册共精选近600个最新热门应用方案，涵盖软件、硬件、数码、平板电脑、手机、网络、网赚、黑客、科技等应用领域。读者不但可以熟知某一主题应用的流程与步骤，还可以从中吸纳别人的成功经验与技巧，从而看之能学，学之能用，用之有效！

超值光盘，收藏必备！

《2013电脑报增刊》光盘又有新突破：

1.**超强装机维护盘**：光盘具备各类维护、优化、检测、安全软件，让你轻松进行装机、系统维护。

2.**更多精彩内容**：光盘中提供正版金山毒霸杀毒软件、苹果热门资源、超值电脑学习视频、丰富PDF电子书、常用工具软件、游戏娱乐等众多资源，方便大家查阅和使用。

瞄准热点，只谈方案，《电脑报2013增刊》，必将为你提升非凡的电脑应用功力，让你轻松跟进IT潮流！

编者

2012.9

光盘精彩导航

黑客攻防视频

安装虚拟机
什么是端口
查看端口
使用SuperScan
打开Telnet连接的后门
防范摄像头木马
黑洞木马开启摄像头
基于ICP漏洞的入侵
揪出隐藏在系统中的木马
开启ICP连接漏洞
利用Telnet入侵
清除Excel密码
清除Word密码
清除压缩文件密码
验证代理
入侵漏洞主机
设置远程协助
远程控制计算机

防火墙与杀毒软件

金山毒霸
金山卫士
瑞星杀毒软件
瑞星个人防火墙
360杀毒
360ARP防火墙
木马专家
反木马卫士
金山ARP防火墙

账号密码保护工具

QQ电脑管家
超级巡警账号保护神
瑞星卡卡上网安全助手
文件密码箱
XP星号密码查看器
360安全卫士
360保险箱

电脑安全辅助工具

360时间保护器
360文件粉碎工具
360系统急救箱
Windows 进程管理器
冰刃
瑞星安全助手
黄山IE修复专家
超级巡警U盘病毒免疫器

黑客攻防电子书

QQ盗号与安全防范
端口与服务攻防实例
多管齐下捍卫你的机密
进程攻防实例解析
信息搜集与扫描
看好你的“钱包”

菜鸟黑客篇

密码安全 你该如何hold住

据报道，2012年4月，一位伊朗黑客为发泄对银行系统的不满，在私人博客上公布了300万张银行卡的卡号和密码，引起当地民众对网络安全的极大担忧。而在国内，也曾相继爆出了CSDN网站密码泄露、人人网、Sina、开心网、百合网、京东商城等一系列密码安全问题……密码安全，大家到底了解多少呢？如何设置安全的密码，如何安全管理密码，本专题将为大家一一揭晓！

强大否？密码安全鉴定……2
一、中外弱密码PK ……2
二、密码安全鉴定 ……2
三、创建强悍密码 ……3
密码管理工具“喜”与“忧”……3
一、不用记？KeePass密码管理工具 …3
1.添加密码 ……3
2.密码管理 ……4
3.生成安全密码 ……4
二、福兮，祸兮？密码软件的隐患 ……5
1.软件安装 ……5
2.密码一览无遗 ……6
3.消除隐患 ……6
另辟蹊径确保文件安全……7
一、“汉字+图片”组合密码 ……7
1.汉字也能做密码 ……7
2.SilentEye图片加密……8
3.文件解密 ……9
二、任意文件均可做密钥 ……9
三、巧借网站实现自动销毁 …… 10
四、X-文件锁保护机密文件 …… 11
五、FileMon监视发现“销毁真相” … 12
六、破解“X-文件锁”加密的文件 … 13
常用密码防破解…… 14
一、密码轻松看网易闪电邮之安全隐患 14
1.网易闪电邮的安全隐患 …… 14
2.安装目录下轻松“获取”密码 …… 15
3.防范之道 …… 16
二、揭秘破解无线路由器密码 …… 16
1.暴力破解无线路由器账号、密码 …… 16
2.修改无线网络密码，免费蹭网 …… 17
三、压缩文档加密与突破 …… 18
1.用RARPasswordCracker恢复密码 …… 18
2.WINZIP压缩文件的破解…… 20
3.WinRAR压缩文件的破解 …… 20

新隐患 智能手机与微博安全防范

伴随智能手机的广泛应用，手机安全问题也日益凸显。据《中国手机安全状况报告》显示，2011年全年新增手机恶意软件及木马8714个，被感染智能手机用户数超过2753万人次。报告同时指出，Android系统成为安全问题最为严重的平台。智能手机都存在哪些安全问题，时下流行的微博是否也暗藏隐患呢？下面将为大家一一介绍。

手机的安全隐患 …… 22

一、手机安全七大问题 …… 22

二、手机骷髅木马 …… 24

善用工具保手机安全 …… 25

一、常用手机安全软件 …… 26

1. 卡巴斯基手机安全软件 …… 26

2. 网秦手机安全卫士 …… 27

二、拦截垃圾短信 …… 27

1. 来电通 …… 27

2.当心“短信群发器”木马 …… 29

三、监控失踪的手机流量 …… 29

1. LBE安全大师 …… 30

2. 扣费病毒伪装热门游戏 …… 31

四、Android病毒不得不防 …… 32

1.一键体检 …… 32

2.病毒查杀 …… 33

五、手机隐私保护 …… 33

微博安全防范 …… 37

一、中奖“钓鱼”陷阱 …… 37

二、微博短链接挂马 …… 38

三、短链接DDOS攻击 …… 38

四、“微博卫士”保微博安全 …… 39

1. 金山微博卫士 …… 39

2. 360微博卫士 …… 40

实战解析 移动存储与图片病毒防范

在各种电脑应用中，图片都是极其常见的数据。优美的风景、巧笑嫣然的美女、风趣幽默的搞怪图片……在享受视图大餐的时候，可曾想过病毒正“破茧而出”，悄悄地透过图片向我们的电脑伸出魔爪？从多年前的软盘感染病毒，到如今的优盘、移动硬盘、光盘传播病毒，移动存储已经成为了危害计算机安全的高危存储介质。在本专题中，将为读者们剖析图片病毒、移动存储病毒的技术原理与防范之策！

Autorun 病毒实战分析 …… 42

一、初识U盘病毒 …… 42

1.什么是U盘病毒 …… 42

2.使用专杀工具剿杀U盘病毒 …… 42

二、Autorun病毒解析 …… 42

1.原理与分析 …… 43

2. 病毒查找 …… 47

3. 病毒清除 …… 47

4. 故障修复 …… 48

U 盘病毒防范之策 …… 48

一、手工方式防U盘病毒 …… 48

二、“防护盒”为U盘护航 …… 51
三、内网当心U盘资料被窃取 …… 53
1.当心黑手“闪盘窥探者” …… 53
2.防范“闪盘窥探者” …… 53

USB 访问权限设置 …… 54
一、禁止安装USB设备的驱动程序…… 54
二、禁用USB存储设备…… 55

图片病毒的制作原理 …… 56
一、什么是图片病毒 …… 56
二、图片病毒的传播方式和原理 …… 56
1.修改文件扩展名 …… 57
2.寄生在压缩包中 …… 57
3.利用漏洞传播 …… 57
4.伪装成BMP图片 …… 58
5.病毒程序使用图片文件图标 …… 59

图片病毒实战解析 …… 59
一、超强免杀图片病毒揭秘 …… 60
二、图片网马实战解析 …… 63

图片病毒防范方法 …… 65
一、安装补丁 …… 65
1.使用“自动更新” …… 66
2.使用第三方程序修补漏洞 …… 66
3.微软网站下载单个补丁 …… 66
二、使用图片病毒专杀工具 …… 66

寻找李鬼 自己动手揪出“黑线”进程

在Windows中，当应用程序运行时将会引发对CPU、内存、硬件设备等系统资源的占用。为了保证系统资源得到合理的分配，Windows使用了“进程”技术对其进行有效管理。所以，任何程序（包括黑客工具或病毒）在运行时，都会有相应的进程！进程是我们查找和清除这些恶意程序的重要线索！在本专题中，就将为读者讲解进程除黑方面的知识。

进程攻防基础知识 …… 68
一、进/线程是干什么的 …… 68
二、怎样分析、关闭和重建进程 …… 72
1. Windows任务管理器 …… 72
2. DOS下管理进程 …… 72

进程攻防实例解析 …… 73
一、如何杀死黑客植入的隐藏进程 …… 73
二、黑客如何查看远程进程 …… 74
三、如何杀死病毒进程 …… 75
四、怎样删除发起进程的恶意程序 …… 77
五、如何查看木马进程对应的服务 …… 78
六、进程的高级管理 …… 78

进程攻防辅助工具 …… 80
一、超级巡警 为系统进程护航 …… 80
1.全面查杀 …… 81
2.实时防护 …… 81
3.保险箱 …… 81
4.系统安全增强工具 …… 82
5.妙用SSDT工具清除流氓软件 …… 82
二、XueTr：超强进程工具 …… 83
1.从进程中发现可疑文件 …… 83
2.查看网络端口与IE插件 …… 84
3.强大的文件管理功能 …… 84
4.服务与启动项管理 …… 85
三、进程、服务藏污垢 察言观色巧识别 85
1.不同颜色显示进程安全级别 …… 85
2.进程比较找出可疑文件 …… 86
3.系统服务也能对比分析 …… 86

时刻警惕 网络盗号与防范实例

如今，网上的应用越来越多，聊天、邮箱、网络游戏、网上银行……这些服务带给大家方便的同时，也让一些盗号者有机可乘。使用的网络服务越多，被盗号的可能性就越大，所以大家必须时刻保持警惕，并掌握一些盗号的防范方法。

QQ 盗号与安全防范 …… 88

一、当心QQ被盗——爱Q大盗 …… 88

1.配置QQ木马 …… 88

2.突破软件的限制 …… 88

3.运行木马，发挥威力 …… 89

二、惊爆！手机QQ不用密码也能登录 89

1.手机QQ漏洞介绍 …… 89

2.手机QQ 漏洞实例演示 …… 89

三、在线盗号的“QQ终结者” …… 90

四、当心通过邮箱盗号：啊拉QQ大盗 92

QQ 权限突破实例解析 …… 94

一、QQ会员、QQ等级任你改 …… 94

1.免费享受QQ会员服务 …… 94

2.QQ等级任你改 …… 95

二、自己动手 尽享VIP版QQ特权 …… 96

1.登录金山快盘 …… 96

2.创建同步文件夹 …… 97

3.聊天记录等数据迁移 …… 98

三、获取QQ空间最高权限 …… 98

四、聊天记录与强制聊天防范 …… 100

1.聊天记录安全 …… 100

2.强行聊天防范 …… 101

其它账号安全防范 …… 103

一、Foxmail账户破解与防范 …… 103

二、网游保镖拒绝盗号 …… 105

1.扫描盗号木马 …… 105

2.保护网络游戏 …… 105

3.保护各种程序 …… 105

4.设置安全规则 …… 106

三、网上银行安全隐患 …… 106

四、网上银行安全防护 …… 107

隐身衣 代理服务器的使用与配置

代理服务器作为黑客入侵的重要工具，对于没有条件多环节反追踪的安全管理人员来说，代理服务器可以切实地起到保护黑客踪迹的作用。在本专题中，将讲解黑客都是如何利用代理服务器进行入侵的，以及什么是IP地址、IP地址是如何得到的、IP地址的追踪与隐藏等方面的知识。

认识 IP、MAC 和域名 …… 110

一、IP地址 …… 110

二、网卡MAC地址 …… 111

三、网站域名 …… 111

IP 地址追踪和隐藏 …… 112

一、获得和追踪IP地址 …… 112

二、隐藏IP地址 …… 113

1. 使用代理服务器 …… 113

2. 使用代理网站 …… 115

三、IP隐藏 让你上网穿件“隐身衣” …116

1.Invisible IP Map …… 116

2.用HSS上美国网站 ……117
3.IP地址隐藏者 ……118

VPN 代理服务器配置 …… 118

一、认识VPN虚拟网 ……119
二、内置拨号配置VPN ……119
三、自动搜索VPN代理 …… 122

攻防实例篇

知己知彼 流行木马攻击与防范要领

从10多年前网民开始接触“冰河”，到现在的技术原理不一、种类繁多的木马大军，木马已经成为黑客入侵和盈利的重要工具。在本专题中，将以几个最流行的木马为例，讲解它们的生成、植入、运作和清除的方法，从而更好地防范木马的入侵。

木马攻防必备基础 …… 124
一、创建“沙盘”测试木马 …… 124
二、木马入侵手法 …… 126
1. 修改图标 ……127
2. 捆绑文件 ……127
3. 定制端口 ……129
4. 文件夹惯性点击 ……129
5. 下载欺骗 ……129

经典木马实战解析 …… 130
一、Xrat木马实战 …… 130
二、灰鸽子 ……131
三、Wollf木马 …… 133
四、免杀木马 …… 135
五、轻松测试EXE文件 …… 137

反弹网页木马攻防 …… 138
一、制作网页木马 …… 138
二、木马效果演示 …… 142
三、木马查杀 …… 144

决胜千里 远程控制实战解析

在所有的黑客行为中，远程控制最为人们所熟悉，也最让网民畏惧。既没有人喜欢鼠标指针被别人随意地点击，也没有人愿意自己的电脑会和陌生人分享管理的权利。那么，远程控制究竟是怎样实现的？在本专题中，就将带领读者们去感受一下远程控制入侵与防范“战场”。

认识远程控制的魅力 …… 146
一、认识远程控制 …… 146
二、多用户远程桌面实战 …… 146

远程控制实例解析 …… 151

一、“屏幕间谍”让你洞悉一切 ……151
1. 屏幕间谍简介 ……151
2.应用实战 ……151
二、UltraVNC轻松遥控远程电脑 … 152
1.被控端（服务器）设置 ……152
2.控制端（客户端）设置 ……153
3.实现远程连接 ……153
命令行远程控制工具 PsTools 154
一、远程登录 …… 154
二、执行命令 …… 156
三、传送文件并执行 …… 156
四、执行远程命令并回显示 …… 156
五、查看远程进程并杀除 …… 158

拒绝被“蹭”无线网络攻防实例

无线网络是近几年来的热门，它已经成为笔记本等电脑中的标配硬件了。无线网络在带来极大便利的同时，也存在着很多安全隐患，其中广为人知的就是容易被“蹭网”。其实，无线网络也有很多安全设计，只不过很多人都不重视。在本专题中，将通过具体的实例带领读者们认识无线安全，并深入学习无线安全策略的配置方法。

认识无线攻击 …… 160
一、无线网络概述 …… 160
二、初识无线攻击 ……161
WEP 加密破解与防范 …… 163
一、无线WEP加密方法 …… 164
二、轻松获取WEP密码 …… 164
三、当心无线WEP被破解 …… 164
1.安装无线网卡驱动 ……165
2.嗅探无线网络数据包 ……166
3.破解WEP密码 ……167
四、防范方法 …… 168
无线网络安全配置 …… 168
一、更改默认设置 …… 169
二、关闭无线路由 …… 169
三、MAC地址过滤 …… 169
四、设置强密码 …… 170

近水楼台 局域网嗅探与网吧攻防解析

输入用户名、密码、服务器地址、信用卡号码等敏感信息，在随着“确定”按钮的点击后，会在网络中进行瞬间的传输。不是专业网络人士的话，绝不会知道黑客在这个过程中就能把信息捕获！无需在目标计算机中植入木马，就能获得重要的信息，这使得嗅探入侵变得神秘异常！在本专题中，将以数个实例讲解局域网和网吧中的安全攻防策略。

局域网嗅探实战 …… 172
一、网络嗅探原理 …… 172
二、邮箱监听实战 …… 174
三、多协议监听实战 …… 175

四、影音嗅探 …… 177

嗅探的应用和防范…… 178

一、网管对嗅探的利用 …… 178

二、怎样防御网络监听 …… 180

剖析网吧安全环境 …… 181

一、安全问题一览 ……181

1.问题一：病毒 ……181

2.问题二：盗号 ……181

3.问题三：网络被攻击 ……182

4.问题四：服务器被入侵 ……182

5.问题五：安全限制被突破 ……182

二、初识防护技术 …… 182

1.还原卡或还原精灵 ……182

2.杀毒软件 ……183

3.网吧管理系统 ……183

突破网吧限制 …… 183

一、手工突破限制 …… 183

二、利用工具破解 …… 185

实例1：读取管理员用户名和密码 ……186

实例2：突破限制 ……186

网吧攻击与防范 …… 186

一、局域网攻击原理 …… 187

二、局域网终结者 …… 187

三、溢出“拿”网吧主机 …… 188

四、网吧安全防范 …… 190

防不胜防 网站挂马与钓鱼解析

目前，网站基本上都是使用动态语句来编写的，因为这样可以极大地减轻网站的整体维护工作量。但是，由于相当多的网站设计师都对安全设计做得不够好，直接引发了URL欺骗、网站挂马等一系列的入侵手段，导致了网站甚至是服务器沦陷。此外，网络钓鱼也层出不穷，令人防不胜防。

动态网站挂马案例剖析 …… 192

一、网站挂马概述 …… 192

二、使用工具批量挂马 …… 192

三、为网站模板添加一句话木马 …… 194

网站挂马防范对策 …… 197

一、检测是否被挂马 …… 197

二、申请安全厂商来保护 …… 198

三、防患于未然 …… 199

网络钓鱼防范对策 …… 199

一、购物类钓鱼网站的特征 …… 199

二、IPAD等热门产品“钓鱼” …… 200

三、医疗、药品类钓鱼网站 …… 200

四、仿“简单百宝箱”的钓鱼网站 … 201

1.简单百宝箱如何被“钓鱼” ……201

2.虚假钓鱼网站实例剖析 ……201

3.检测百宝箱是否正版 ……202

安全防范篇

安全为上 系统账户与口令攻防

系统登录密码是电脑安全的第一道防线，也是非常关键的一道壁垒，但系统口令往往也常有被破解的情况。下面将以主流的WinXP、Win7、Win8系统为例，看看系统口令是如何被破解的，并介绍相应防范技巧。

认识 XP 系统密码破解 …… 204

一、初识系统密码 …… 204

1.从XP登录过程看密码安全 ……204

2.XP中账户管理 ……205

二、木马攻破XP密码 …… 207

恢复、重设和清除 XP 密码 211

一、密码恢复功能 ……211

二、ERD Commander重设密码 … 212

三、清除密码 …… 213

四、密码的安全管理 …… 215

Win7 登录口令破解与恢复 … 216

一、重置账户密码 …… 216

二、清除账户密码 …… 217

三、直接查看系统登录密码 …… 218

登录 SYSTEM 账户获取最高权限 219

一、命令行登录SYSTEM账户 …… 220

二、SYSTEM账户下的“特权” … 220

Win8 安全不走寻常路 …… 221

一、“系统刷新”让Ghost靠边站 … 222

二、创建“系统映像”保安全 …… 222

三、“系统刷新”快速重装系统 …… 223

四、“系统重置”也简单易用 …… 224

网络暴力 拒绝服务和网络炸弹攻防

有时候，当我们在浏览网页，准备查找所需要的信息时，突然卡机或网络断线；打开邮箱准备收信，却发现邮箱里面灌满了垃圾邮件；在论坛上正和朋友们聊得欢，突然发现有人正冒充我们的名字大放厥词……以上种种，可能是中了网络炸弹所致。在本专题中，将会介绍各种网络炸弹和拒绝服务的防御方法。

认识网络炸弹…… 226

一、什么是网络炸弹 …… 226

二、炸弹的分类 …… 227

炸弹攻防实例 …… 229

一、蓝屏炸弹 …… 229

二、Ping轰炸防范…… 230

三、UDP攻击 …… 232
四、蜗牛炸弹 …… 232

DoS 拒绝服务攻防 …… 233

一、DoS攻击手法 …… 233
二、目标的确定 …… 235
三、常见工具应用 …… 237
1. DDoS Ping …… 237
2. TCP连接轰炸 …… 238
3. P2P轰炸机 …… 238

直击核心 论坛与数据库攻防实战

只要是涉及数据库的网站或软件，数据库都是核心！只要数据库中的重要内容能够被黑客读取，那么就等同于把最高权限拱手相让。因此，数据库的安全一直都是服务器和网站防黑设计中的重中之重！本专题中，将讲解主流的几种数据库的入侵与防范技术。

主流论坛攻防实战解析 …… 240

一、Discuz 7.X入侵与防范 …… 240
二、轻松暴库动网 …… 242
三、终极注入PHPWind …… 243

数据库的重要性何在 …… 245

一、数据库是什么 …… 245
二、黑客是如何找到数据库的 …… 245

SQL 攻击实例解析 …… 246

一、SQL溢出实战 …… 246
二、SQL弱口令扫描 …… 248
三、SQL 注入 …… 249
四、数据库密码暴力猜解 …… 249

数据库防范秘技 …… 250

一、本机中的数据库安全策略 …… 250
二、购买空间的安全策略 …… 250
三、特殊文件名法 …… 251

千防万护 服务器入侵与防范解析

服务器存在的根本目的就是向用户提供各种服务和数据，这就决定了它的防守有一个限度，太严格了会制约用户的使用，太开放了就会带来极大的隐患。所以，服务器很容易就会因为安全配置不当产生一些漏洞。很多服务器漏洞可以让黑客对其中存储的各种数据（如网站、论坛）产生致命的影响。在本专题中，就将讲解几种主流的服务器入侵和防范技术。

服务器安全与漏洞检测 …… 254

一、服务器安全概述 …… 254
二、服务器的漏洞侦测 …… 255

MS08-067 服务器漏洞攻防 256

一、攻击原理 …… 256
二、攻击实战解析 …… 257

三、安全防范 …… 259

CC攻击实战解析 …… 261

一、攻击原理 …… 261
二、攻击实例分析 …… 262
三、识别CC攻击 …… 263
四、轻松抵御CC攻击 …… 264
1.第一条规则 ……265
2.第二条规则 ……265
3.第三条规则 ……266
4.第四条规则 ……266

服务器安全配置 …… 267

一、安装补丁 …… 267
二、权限设置 …… 268
三、删除LAN设置 …… 269

杜绝隐患 入侵检测与日志管理

如果有人问你的系统是否安全？你该如何作答？是毫无所知，还是一筹莫展？其实，回答这个问题的最好办法就是学会入侵检测技术！如果能熟练地掌握这项技术，就可以将危险屏蔽在系统之外！在专题中，就将讲解主流的入侵检测与安全配置技术！

认识入侵检测系统 …… 272

一、入侵的定义 …… 272
二、入侵检测的起点 …… 272
三、入侵检测基本模型 …… 273
四、按照信息源的分类 …… 273

入侵检测实战操作 …… 274

一、用X-Scan检测目标主机 …… 274
二、IIS Lock Tool扫描服务器 …… 276
三、防范扫描攻击 …… 278
1. 端口防范 ……278
2. 安装补丁 ……282

日志安全管理 …… 282

一、日志概述 …… 283
二、安全日志的启用 …… 286
三、四项基本技能 …… 287
1. 事件筛选 ……287
2. 查找记录 ……287
3. 排序事件 ……288
4. 新建查看 ……288
四、清除与保存日志 …… 288
1. 本地清除 ……288
2. 保存日志 ……289
3. 远程清除 ……289
4. 清除IIS日志 ……290

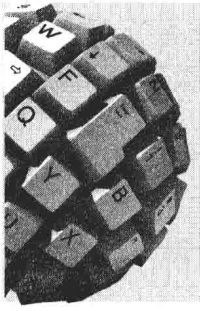
电脑报增刊

POPULAR COMPUTERWEEK NO.01

电脑报官方网站：www.icpcw.com
电脑报官方书博：weibo.com/bookpub

密码安全

你该如何hold住



据报道，2012年4月，一位伊朗黑客为发泄对银行系统的不满，在私人博客上公布了300万张银行卡的卡号和密码，引起当地民众对网络安全的极大担忧。而在国内，也曾相继爆出了CSDN网站密码泄露、人人网、Sina、开心网、百合网、京东商城等一系列密码安全问题……密码安全，大家到底了解多少呢？如何设置安全的密码，如何安全管理密码，本专题将为大家一一揭晓！

精彩看点

- 汉字也能做密码
- SilentEye图片加密
- 暴力破解无线路由器密码
- 破解“X-文件锁”
- 密码恢复技巧

专题导航

强大否？密码安全鉴定

一、中外弱密码PK

二、密码安全鉴定

三、创建强悍密码

密码管理工具“喜”与“忧”

一、不用记？KeePass密码管理工具

二、福兮，祸兮？密码软件的隐患

另辟蹊径确保文件安全

一、“汉字+图片”组合密码

二、任意文件均可做密钥

三、巧借网站实现自动销毁

常用密码防破解

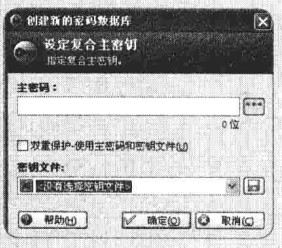
一、网易闪电邮之安全隐患

二、揭秘破解无线路由器密码

三、压缩文档加密与突破

强大否？密码安全鉴定 P002

提到密码安全，很多朋友可能都会想到：要保管好自己的密码，不要让第三方窥视；要设置尽量复杂的密码，不要使用自己的生日做密码；不要使用简单的英文单词做密码……只知道这些还不够，什么样的密码才够强大，如何查看密码是否强大，很多人并不知道。



密码管理工具“喜”与“忧” P003

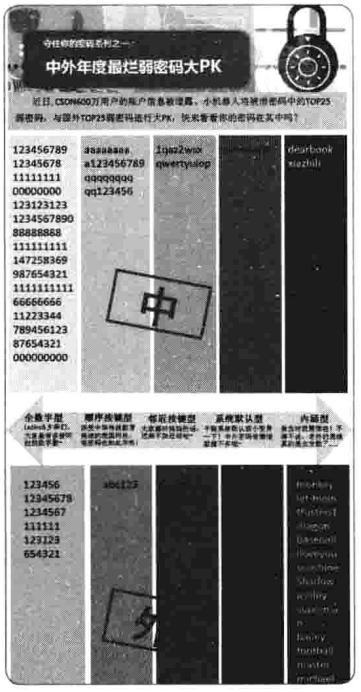
前面，我们解决了密码安全强度的问题，但接下来一个新的问题产生了：根据密码安全的规则，尽量使用复杂的密码，而且建议大家在不同的网站、论坛、邮箱使用不同的密码，如此多而复杂的密码，又怎能记得住呢？这时，密码管理软件粉墨登场。

强大否？密码安全鉴定

提到密码安全，很多朋友可能都会想到：要保管好自己的密码，不要让第三方窥视；要设置尽量复杂的密码，不要使用自己的生日做密码；不要使用简单的英文单词做密码……只知道这些还不够，什么样的密码才够强大，如何查看密码是否强大，很多人并不知道。

一、中外弱密码PK

首先我们看看参考金山公司为大家总结的“中外年度最烂弱密码大PK”（http://weibo.com/1642668915/xDd6i2hPf），此微博页面中，金山将被泄露密码中的TOP25弱密码，与国外TOP25弱密码进行大PK，你是否也有这类弱密码呢，如果有，请千万要避开。



二、密码安全鉴定

当然，也许你的密码没有上面罗列的那么“弱智”，但安全强度到底如何呢，我们可以借用工具软件来检测。这里给大家推荐一款“密码安全鉴定器”，这是由360公司推出的一款密码安全鉴定工具，可以有效地帮助大家检测密码是否安全。

“密码安全鉴定器”内嵌于360安全卫士中，下载并安装最新的360安全卫士，然后只需要点击“功能大全”即可看到该工具。点击“密码安全鉴定器”，在打开的窗口中只要输入你要鉴定的密码，然后点击“检测”即可查看密码的安全等级。

如果是纯数字的密码，密码安全等级得分很低，相反如果有数字、字母（大小写混用）、符号的组合，则密码安全等级更高。