

15个精彩专题 150套完整方案 2000幅直观图解

# 电脑报增刊

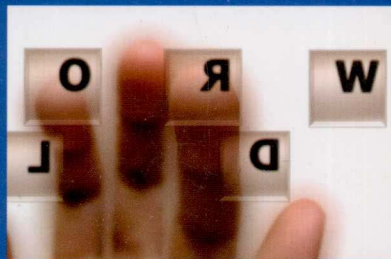
## 2012ZENGKAN

### 网络攻防与电脑安全年度应用方案

电脑报 编

#### 密码/破解/隐写术

解除封锁 黑客常用破解招式解析  
突破软件“注册”的封锁  
文件“自动销毁”与破解  
“栽”后即焚：机密文档传输  
鲜为人知的“隐写术”加密



#### 挂马/漏洞 远程监控

简单百宝箱反钓鱼实战  
“网络人”内网外网全拿下  
E盾：另类教你玩“监控”  
博客程序L-BLOG攻防



#### 中奖/盗号/防欺诈

短链、秒杀器 微博与网购安全隐患  
逃无可逃 QQ盗号与防范  
QQ系统假消息制作揭秘  
QQ申诉也被黑客利用  
“QQ防骗技巧”暗藏新骗局



#### 扫描/嗅探/信息筛选

黑客社会工程学搜集信息  
信息安全保卫战 拒绝做“肉鸡”  
扫描目标主机与漏洞  
用ProtectX防御扫描器追踪  
网络监听实战解析

#### 网游/网吧/网站攻防

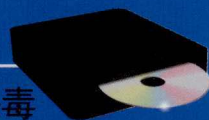
快乐背后 网络游戏攻防实例  
网吧ARP欺骗实例解析  
网站常见攻击方式解密  
严格账户管理保服务器安全

#### 端口/无线/病毒防范

守住入口 进程与端口攻防解析  
3389端口入侵与防范  
无线WEP加密破解与防范  
隐患重重 无线网络破解与安全防范  
当心“美人计” 图片网马实战解析

### 超值光盘

《金山毒霸》《瑞星杀毒软件》永久免费 专业杀毒



电脑安全攻防必备工具 苹果热门资源集  
黑客攻防学习资源 十大黑客电影介绍

视频、电子书等学习资源集  
游戏资源、主题壁纸、音乐电影 丰富有趣

# 电脑报 增刊

2012ZENGKAN

网络攻防与电脑安全年度应用方案

电脑报 编

## 内容提要

精选15大热门黑客攻防专题，包含200多个热点应用方案，1000余条攻防技巧，为大家解析黑客的各种攻防技术和攻防手段，并介绍行之有效的防范措施。具体内容包括：微博与网购安全隐患、QQ盗号与防范、扫描与嗅探、端口与进程攻防、加密与突破、网络钓鱼与网页挂马、网络游戏攻防、网吧入侵与防范、图片病毒攻防、无线网络攻防、网站与服务器攻防等。

《2012电脑报增刊——网络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。全手册方案详尽，实用性强，适合广大初、中级电脑安全爱好者及安全管理人员阅读与收藏。

**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！

版权所有	盗版必究
未经许可	不得以任何形式和手段复制和抄袭

## 2012电脑报增刊——网络攻防与电脑安全年度应用方案

编 著：电脑报

责任编辑：李 勇

版式设计：程 佳

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

C D 生 产：四川省葭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

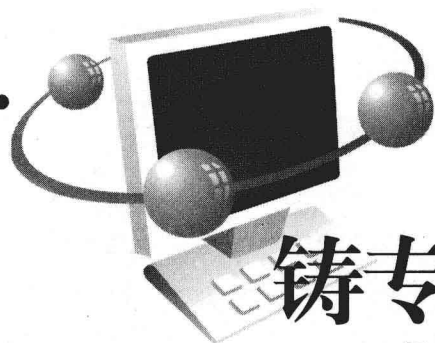
版 号：ISBN 978-7-89476-676-2

版 次：2011年10月第1版 2011年10月第1次印刷

定 价：35.00元（1CD+手册）

本出版物所使用方正字体经方正授权许可





电脑报增刊

Preface

# 铸专题聚年度热点 撰方案解应用难题

- 电脑报年度大作 10年持续畅销图书 ● 完全聚焦热点 只谈实用方案 IT应用全“Hold”住
- 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……

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, 那么, 掌握热门的电脑与数码应用方案, 精通各种使用技巧, 那是必须的! 纵然有海阔天空的网络资源, 即使有高手朋友帮你解决难题, 都不如打开这套《2012电脑报增刊》, 方案握在手, 排困不求人。

**因为专注, 所以专业!**

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250万册, 直接和间接读者估计超过500万人。《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。

**因有特色, 非看不可!**

1. **独立专题, 紧扣热点:** 《2012电脑报增刊》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:** 《2012电脑报增刊》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!

**因为超值, 收藏必备!**

《2012电脑报增刊》光盘又有新突破:

1. **众多学习资源:** 光盘中提供了30多个电脑安全学习资源和黑客攻防视频资源, 让大家轻松掌握黑客攻防要领。

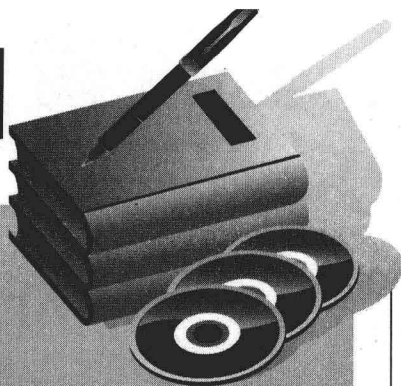
2. **超值精彩内容:** 光盘中提供正版金山毒霸杀毒软件、精彩丰富的苹果热门资源、电脑报阅读系统、丰富PDF电子书、常用工具软件、游戏娱乐等众多资源。

**瞄准热点, 只谈方案, 《2012电脑报增刊》, 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

2011.10

# 光盘精彩导航



超值赠送

永久免费 专业杀毒 全面安全防护

## 《金山毒霸》

- 30核云引擎
- 99秒云鉴定
- 独家边界防御

## 《瑞星杀毒软件》

- 系统内核加固
- 木马防御
- U盘防护
- 浏览器防护
- 办公软件防护

## § 电脑安全攻防必备工具

- 文件密码箱
- 瑞星卡卡上网安全助手
- 可牛盗号木马专杀工具
- 金山卫士
- 金山ARP防火墙
- 超级巡警账号保护神
- 超级巡警U盘病毒免疫器
- 冰刃
- Windows 进程管理器
- QQ电脑管家
- 360系统急救箱
- 360文件粉碎工具
- 360时间保护器
- 360保险箱
- 360安全卫士

## § 黑客攻防视频

- 安装虚拟机
- 查看端口
- 打Telnet开连接的后门
- 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
- 清除Excel密码

- 清除Word密码
- 清除压缩文件密码
- 设置远程协助
- 使用SuperScan
- 远程控制计算机
- .....

## § 苹果热门资源集

- 壁纸
- 铃声
- 主题
- 软件: CallClear、FreeRapid、Good\_Reader、MobileRSS、QQ、SyncInABlink

## § 电脑安全学习资源

- 3389端口入侵与防范
- IE7 ODAY漏洞攻防实例
- QQ聊天中的几大陷阱
- QUICKIP进行多点远程控制
- 常见木马入侵手法
- 打造一键GHOST恢复系统
- 缓存溢出工具
- 局域网环境下的安全隐患
- 屏幕间谍定时抓屏监控
- 如何快速判断电脑是否中毒
- 扫描端口保护电脑安全
- 网站攻防基础知识
- 系统密码的设置与解除
- 信息筛选有诀窍
- 用WINVNC实现远程控制
- .....

## § 十大黑客电影介绍

- 《黑客》
- 《黑客帝国》
- 《剑鱼行动》
- 《杀人硬件》
- 《天才除草人》
- 《通天神偷》
- 《网络惊魂》
- 《异次元黑客》
- 《约翰尼记忆术》
- 《战争游戏》



# 菜鸟黑客篇

## 中奖、短链、秒杀器 微博与网购安全隐患

当前，网上最热门的应用非微博和网购莫属了。哪里有人气，哪就有“黑客”的身影，在热闹的背后，你可曾注意到微博和网购面临的诸多安全陷阱？中奖诱惑、短链接挂马、带毒的淘宝秒杀器、真假难辨的钓鱼网站、防不胜防的团购诈骗、伸向网上支付的黑手……对于广大网民来讲，这些直接关系到大家的切身利益，你不可不防！本专题就带领大家认识微博和网购、团购中的安全隐患，并做好相应的防范工作。

<b>微博安全“三隐患”</b> .....	2	三、医疗、药品类钓鱼网站 .....	7
一、中奖“钓鱼”陷阱 .....	2	<b>团购诈骗：低价购物你不得不防</b> .....	7
二、微博短链接挂马 .....	2	一、价格悬殊太大“靠不住” .....	8
三、短链接DDOS攻击 .....	3	二、团购网站赔付、保障要看清 .....	8
四、“微博卫士”保微博安全 .....	3	三、团购网资质、实力要关注 .....	8
1. 金山微博卫士 .....	4	四、利用互联网搜集“民意” .....	9
2. 360微博卫士 .....	4	<b>网上购物支付选好“中介”</b> .....	9
<b>当心带毒“秒杀器”</b> .....	5	一、银行汇款玩失踪 .....	9
一、金山卫士网页防护 .....	5	二、虚假银行汇款单骗店主 .....	10
二、金山卫士下载后查毒 .....	5	三、简单设置增强支付宝安全性 .....	10
三、金山毒霸实时防毒 .....	6	<b>金山毒霸 2011 捍卫网购安全</b> .....	11
<b>当心被网站“钓鱼”</b> .....	6	一、钓鱼、恶意网站拦截 .....	11
一、购物类钓鱼网站的特征 .....	6	二、网上支付：网购保镖为你把关 .....	12
二、iPhone等热门产品的钓鱼网站 .....	6	三、拦截网购木马，网购不中毒 .....	12

## 解除封锁 黑客常用破解招式解析

在电脑使用中，很多操作都涉及到密码，比如系统密码、无线上网密码、压缩文档密码等，如果密码遗忘了，有没有解除的办法呢？对于一些共享软件，常常有使用次数、使用时间以及功能的限制，是否有办法突破呢？本专题将为大家分析常用的破解招式。



<b>突破“密码”的限制</b> .....	<b>14</b>
<b>一、当心系统密码被破解</b> .....	<b>14</b>
1.Syskey双重加密.....	14
2.轻松创建“开机软盘” .....	14
<b>二、解除NOD32的密码保护</b> .....	<b>15</b>
1.NOD32个人密码设定 .....	15
2.修改注册表清除密码 .....	15
3.使用专用工具“解锁” .....	16
<b>三、破解路由器无线蹭网</b> .....	<b>16</b>
1.解除无线路由器账号、密码 .....	16
2.修改无线网络密码，免费蹭网 .....	17
<b>四、压缩文档加密与突破</b> .....	<b>17</b>
1.RAR Password Cracker恢复密码.....	18

2.“多功能密码破解软件”恢复密码 .....	19
3.破解压缩文件密码 .....	20

### 突破软件“注册”的封锁..... 21

<b>一、解除软件使用次数限制</b> .....	<b>22</b>
<b>二、解除软件使用时限</b> .....	<b>23</b>
<b>三、突破“注册码”限制</b> .....	<b>26</b>

### 其他突破方式..... 28

<b>一、光盘隐藏文件功能的破解</b> .....	<b>28</b>
<b>二、突破软件下载限制</b> .....	<b>29</b>
1.突破“专用下载通道”限制 .....	29
2.金山游侠突破QQ旋风连接限制.....	30

## 密码安全 各类新奇招式巧设密码

加密，历来是大家用来保护机密的一种手段，然而加密被人识破后就很容易被破解，这里将为大家介绍一些新奇的加密招式，比如让文件“蒸发”、文件阅读后“自动销毁”、鲜为人知的“隐写术”、系统登录密码变“动态”等。

### 简单几步让文件夹彻底“消失”... 34

<b>一、更改文件夹图标</b> .....	<b>34</b>
<b>二、隐藏文件名</b> .....	<b>34</b>
<b>三、更改特殊文件名</b> .....	<b>35</b>
<b>四、巧用“文件更名”让文件“蒸发”</b> ...	<b>35</b>

### 文件“自动销毁”与破解..... 36

<b>一、巧借网站实现自动销毁</b> .....	<b>36</b>
<b>二、软件让你保护机密文件</b> .....	<b>37</b>
<b>三、FileMon监视工具发现“真相”</b> .....	<b>38</b>
<b>四、提取“X-文件锁”加密的文件</b> .....	<b>39</b>
<b>五、“载”后即焚：机密文档传输</b> .....	<b>40</b>
1.注册iwormhole用户 .....	40
2.发送文件 .....	40
3.下载文件 .....	41

### 鲜为人知的“隐写术”加密..... 41

<b>一、什么是隐写术</b> .....	<b>42</b>
<b>二、使用二维码“隐写”</b> .....	<b>42</b>
<b>三、使用图片“隐写”</b> .....	<b>43</b>

### 文件加密与破解妙招..... 44

<b>一、另辟蹊径让杀毒软件“藏”机密</b> .....	<b>44</b>
1.杀毒软件的副业——“文件隐藏” .....	44
2.机密文件提取——“文件恢复” .....	45
3.机密文件不泄密——关闭自动上传 .....	45
<b>二、让加密软件形同虚设</b> .....	<b>46</b>
1.文件夹加密测试 .....	46
2.文件夹嗅探器让加密形同虚设 .....	46

### 另类方式为系统和电脑加密..... 47

<b>一、系统登录密码变“动态”</b> .....	<b>47</b>	3. 开机锁实测 .....	50
1. 软件基本设置 .....	47	<b>三、LockItTight找回丢失的电脑</b> .....	<b>50</b>
2. 设置密码卡 .....	48	1. LockItTight网站注册 .....	50
3. 使用动态密码登录系统 .....	48	2. LockItTight软件登录 .....	51
<b>二、U盘变身开机“锁”</b> .....	<b>49</b>	3. 设置追踪的信息 .....	51
1. 巧用shutdown命令 .....	49	4. 查看被盗机器的信息 .....	51
2. 修改组策略, 添加启动项 .....	49		

## 不可或缺 信息搜集与筛选实例

在黑客攻防中, 信息搜集是一项非常重要的工作: 从攻的角度看, 需要了解被攻击机器的操作系统、漏洞情况、端口开放情况等; 而从防的角度看, 我们必须隐藏好自己的电脑相关信息, 比如IP地址、个人QQ、甚至包括博客信息等。本专题将为大家一一剖析信息搜集与防范的要领。

<b>搜集操作系统相关信息</b> .....	<b>54</b>	<b>二、黑客社会工程学的常用手段</b> .....	<b>63</b>
<b>一、X-scan搜集操作系统版本</b> .....	<b>54</b>	1. 电话中的骗术 .....	64
1. X-Scan介绍 .....	54	2. 利用社交网站 .....	64
2. 探测步骤 .....	54	3. “输入错误”也被利用 .....	64
<b>二、Ping命令探测操作系统</b> .....	<b>55</b>	4. 精说行话 .....	64
1. 使用Ping命令探测 .....	55	5. “十度分隔法”获取信息 .....	64
2. 通过网站判断 .....	56	<b>三、从QQ、博客中挖掘信息</b> .....	<b>65</b>
<b>探测漏洞及网站信息</b> .....	<b>57</b>	1. 挖掘你需要的QQ号 .....	65
<b>一、搜索特殊的“关键词”</b> .....	<b>57</b>	2. 通过博客挖掘更多信息 .....	65
<b>二、Google Hacker威力无穷</b> .....	<b>58</b>	3. 从QQ开始“探路” .....	66
<b>三、网站也会让你泄密</b> .....	<b>58</b>	4. 不容忽视的QQ群 .....	67
1. 域名基础知识 .....	58	<b>信息筛选有诀窍</b> .....	<b>67</b>
2. 探测域名与IP .....	59	<b>一、人工筛选信息</b> .....	<b>68</b>
3. 用Nslookup命令查询IP相关信息 .....	60	<b>二、软件筛选信息</b> .....	<b>69</b>
4. 获得网站基本信息资料 .....	61	<b>信息安全保卫战拒绝做“肉鸡”</b> ...	<b>70</b>
5. 查看网站备案登记信息 .....	62	<b>一、什么是“肉鸡”</b> .....	<b>70</b>
6. 查看网站其他信息 .....	62	<b>二、如何判断电脑是否成为“肉鸡”</b> .....	<b>71</b>
<b>黑客社会工程学搜集信息</b> .....	<b>63</b>	<b>三、使用工具软件检测是否为“肉鸡”</b> ...	<b>72</b>
<b>一、什么是社会工程学</b> .....	<b>63</b>	1. 使用Tcpview检测网络连接 .....	72
		2. 使用“金山肉鸡检测器” .....	72





# 扫描嗅探篇

## 守住入口 进程与端口攻防解析

Windows进程和端口是很多用户最容易忽略的，可能甚至有的新用户都不知道他们的存在。然而，进程和端口在系统安全中起着非常重要的作用，黑客常常会利用系统开放的端口入侵你的电脑，因此，不是必须开启的端口应该尽量关闭。而黑客或者病毒恶意程序入侵你的电脑后，通常会在系统进程中有所体现，所以，把好进程关则可以很好地防范黑客和各种有害程序。

### 认识 Windows 进程 ..... 74

- 一、关闭进程和重建进程 ..... 74
  - 1. 关闭进程 ..... 74
  - 2. 新建进程 ..... 74
- 二、查看进程的发起程序 ..... 75
- 三、关闭任务管理器杀不了的进程 ..... 75
  - 1. 哪些系统进程可以关掉 ..... 75
  - 2. 关闭任务管理器杀不了的进程 ..... 76
- 四、查看隐藏进程和远程进程 ..... 76
  - 1. 查看隐藏进程 ..... 76
  - 2. 查看远程进程 ..... 76
- 五、杀死病毒进程 ..... 77

### 当心病毒寄生 SVCHOST.EXE 中 78

- 一、认识SVCHOST.EXE..... 78
- 二、识别SVCHOST.EXE进程中的病毒 78

### 判断 Explorer.exe 进程真假 ..... 79

- 一、什么是Explorer.exe进程 ..... 79
- 二、Explorer.exe容易被冒充 ..... 79

### 进程安全辅助工具..... 80

- 一、巧用Windows 进程管理器 ..... 80
  - 1. 进程管理 ..... 80

- 2. 恶意进程分析 ..... 81

### 二、超级巡警保护系统进程 ..... 81

- 1. 全面查杀 ..... 81
- 2. 实时防护 ..... 82
- 3. 保险箱 ..... 82
- 4. 系统安全增强工具 ..... 82
- 5. 妙用SSDT工具清除流氓软件 ..... 83

### 三、堪比兵刃的超强手工杀毒辅助工具 ... 84

- 1. 从进程中发现可疑文件 ..... 84
- 2. 查看网络端口与IE插件 ..... 85
- 3. 强大的文件管理功能 ..... 85
- 4. 服务与启动项管理 ..... 85

### 系统端口基本操作..... 86

#### 一、端口的分类 ..... 86

- 1. 已知端口 ..... 86
- 2. 注册端口 ..... 86
- 3. 动态端口 ..... 86

#### 二、开启和关闭端口 ..... 87

- 1. 查看端口 ..... 87
- 2. 关闭端口 ..... 87
- 3. 开启端口 ..... 87

#### 三、端口查看工具 ..... 87

#### 四、重定向本机默认端口 ..... 88

1.在本机上(服务器端)修改 .....	88
2.在客户端上修改 .....	89
<b>3389 端口入侵与防范 .....</b>	<b>89</b>
一、什么是3389端口 .....	89
二、3389入侵实例剖析 .....	90
三、3389端口安全防范 .....	90
<b>扫描端口确保电脑安全.....</b>	<b>91</b>

一、常见端口剖析 .....	91
二、用SuperScan扫描端口安全 .....	92
三、用NetBrute Scanner扫描端口 .....	92
<b>创建安全策略过滤与禁止 135 端口 ...</b>	<b>93</b>
一、创建IP筛选器和筛选器操作 .....	93
二、创建IP安全策略 .....	95
三、指派和应用IPsec安全策略 .....	96

## 逃无可逃 QQ盗号与防范

随着QQ用户的增多,针对QQ的各类骗局和攻击也越来越多:QQ盗号、强制视频聊天、偷窥聊天记录、Q币安全……这些都让我们不得不防!QQ开启的各项服务越多,也就面临更多的安全隐患,需要大家不断完善配置,随时提防各类骗术!

<b>当心针对 QQ 的各类骗局 .....</b>	<b>98</b>
<b>一、QQ系统假消息制作揭秘 .....</b>	<b>98</b>
1.QQ系统消息制作揭秘.....	98
2.QQ系统假消息实例演示.....	98
3.如何防范QQ系统假消息.....	99
<b>二、解析收文件QQ被盗的骗局 .....</b>	<b>99</b>
1.盗号骗局再现 .....	99
2.双格式文件实例解析 .....	100
3.防盗技巧 .....	100
<b>三、当心“QQ靓号”诱惑你 .....</b>	<b>101</b>
1.“QQ靓号”的诱惑.....	101
2.安全防范技巧 .....	102
<b>四、“最新刷Q币”的骗局 .....</b>	<b>102</b>
1.骗术现场 .....	102
2.骗术解析 .....	103
3.防骗技巧 .....	104
<b>五、“QQ防骗技巧”暗藏新骗局 .....</b>	<b>104</b>
<b>QQ 强制聊天与聊天记录攻防 ...</b>	<b>105</b>

<b>一、QQ强制视频聊天 .....</b>	<b>105</b>
1.强制视频聊天解析 .....	105
2.防范技巧 .....	106
<b>二、QQ聊天记录攻防 .....</b>	<b>106</b>
1.聊天记录防范 .....	106
2.强行聊天防范 .....	107
<b>QQ 盗号与安全防范 .....</b>	<b>108</b>
<b>一、爱Q大盗盗号解析 .....</b>	<b>108</b>
1.配置QQ木马.....	108
2.突破软件的限制 .....	109
3.运行木马 .....	109
<b>二、QQ申诉也被黑客利用 .....</b>	<b>109</b>
1.木马客户端制作解析 .....	110
2.QQ密码很容易被盗.....	110
3.QQ申诉信息“夺取”QQ号 .....	111
4.防范技巧 .....	111
<b>三、为QQ硬盘设置密码 .....</b>	<b>111</b>
<b>四、为QQ通讯录设置密码 .....</b>	<b>112</b>
<b>五、看好你的Q币 .....</b>	<b>112</b>



**六、使用密保卡保护QQ ..... 113**

- 1. 认识密保卡 ..... 113
- 2. QQ密保卡使用方法 ..... 113

**七、QQKav轻松搞定聊天安全 ..... 115**

- 1. 多种杀毒方式，让你远离病毒 ..... 115
- 2. 快速找出进程、服务中的可疑项 ..... 116
- 3. 轻松屏蔽恶意网站、欺诈信息 ..... 116

**快乐背后 网络游戏攻防实例**

据统计，2010年互联网游戏用户总数突破1.2亿人，同比2009年增长超过37%，而在2011年，网络游戏用户还将继续猛增。在庞大的用户背后，随之而来的也有很多不和谐的声音：游戏账号被盗、装备被窃取、游戏用户遭遇网络钓鱼、木马外挂满天飞……网络游戏给大家带来快乐的同时，一些不法分子也将黑手伸向了网游，你不可不防！

**几种常见的游戏攻击手段 ..... 118**

- 一、游戏存在的安全隐患 ..... 118
- 二、游戏外挂 ..... 119
- 三、游戏中暗藏木马 ..... 120
- 四、游戏密码保护 ..... 121
- 五、针对游戏的网络钓鱼 ..... 122
- 六、游戏中防欺诈 ..... 124

**借助安全工具防范游戏攻击 ..... 125**

- 一、用可牛免费杀毒软件增强安全 ..... 125
  - 1. 联手卡巴斯基，双管齐下杀病毒 ..... 125

- 2. 实时防护，给你全方位保护 ..... 126
- 3. 高级防御，网页、邮件齐监控 ..... 126

**二、密保卡保护 防盗号就用“巨盾” ..... 127**

- 1. 全面掌控系统安全 ..... 127
- 2. 三种方式查杀木马 ..... 128
- 3. 首创“密保卡”方式防盗号 ..... 128
- 4. 保险箱让账号更保险 ..... 129

**三、用奇虎360保险箱防盗号 ..... 130**

- 1. 安全启动软件 ..... 130
- 2. 查看正在保护的软件和保护历史 ..... 130
- 3. 360保险箱个性设置 ..... 130

**隐患重重 无线网络破解与安全防范**

无线网络以其方便性和灵活性深得广大用户的厚爱，近年来，使用无线网络的用户也越来越多。很多家庭和企业都配置了无线网络，而且很多公共场所都可以免费无线上网，比如机场、咖啡厅等。伴随无线网络应用的增多，无线网络安全问题也日益凸显，无线网络被盗用的情况时有发生，而且最可怕的是无线网络加密也被破解，那么使用无线网络，应该如何才能确保高效、安全呢？应该如何防范？下面与大家一起分享。

**无线网络的安全隐患 ..... 132**

- 一、信号被盗：为别人买单 ..... 132

- 1. 情况描述：高额网费 ..... 132
- 2. 解决办法：WEP加密 ..... 132

二、修改组策略防范会议大厅数据被盗用	133	WPA 加密破解与防范	139
1. 修改组策略禁止空密码访问	133	一、WPA、WEP无线加密对比	139
2. 使用无线AP进行端口隔离	133	二、WPA加密被破解后的安全措施	140
三、在无线局域网中“隐身”	133	1. 第一步：使用WPA2方式来加密	140
1. 修改编辑注册表	133	2. 第二步：为WPA/WPA2设置复杂密码	140
2. 输入“隐藏”命令	133	3. 第三步：WAPI协议作为辅助手段	140
四、禁止部分人上网	134	消除无线安全隐患的8种手段	141
无线 WEP 加密破解与防范	134	一、隐藏SSID	141
一、无线WEP加密方法	134	二、MAC地址过滤	141
二、轻松获取WEP密码	134	三、WEP加密	141
三、当心无线WEP被破解	135	四、WPA加密	142
1. 安装无线网卡驱动	135	五、WPA2加密	142
2. 嗅探无线网络数据包	136	六、AP隔离	142
3. 破解WEP密码	138	七、802.1x协议	142
四、防范方法	138	八、802.11i	142

## 三板斧 网络扫描、嗅探与监听实例分析

在黑客攻防中，有很多敏感信息、弱口令等都是黑客非常喜欢的，而要获取这些信息，需要借助一些扫描、监听工具才能实现，本专题将为大家介绍黑客常用的扫描、嗅探工具，并为大家介绍相应的防范之策。

扫描目标主机与漏洞	144	一、Iris嗅探捕获数据	151
一、Sss扫描器扫描实战	144	1. 捕获数据	152
1. 什么是扫描	144	2. 分析数据	152
2. 扫描实战	144	3. 信息过滤	152
二、流光扫描弱口令	147	4. 流量测试	153
1. 流光简介	147	5. 怎样防御嗅探器	153
2. 批量主机扫描	147	二、无线嗅探器：NetStumbler	153
3. 指定漏洞扫描	149	1. 无线安全很重要	154
三、用ProtectX防御扫描器追踪	150	2. 应用实战	154
1. ProtectX实用组件解析	150	3. 拒绝笔记本ad-hoc方式接入	155
2. 防御扫描器攻击	151	三、命令行下的嗅探器WinDump	156
当心工具嗅探机密数据	151	1. 魅力所在	156
		2. 应用实战	156





网络监听实战解析.....	158	三、网络监听防范方法 .....	163
一、监听的魅力 .....	158	四、妙用蜜罐诱敌深入 .....	163
二、监听实战分析 .....	161	1.什么是蜜罐 .....	163
		2.个人级蜜罐系统的实现 .....	164

## 攻防实例篇

### 当心“美人计” 图片病毒的原理与识别

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、感人至深的图解、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？在本专题中，将为读者们剖析图片病毒的技术原理、制作方法与防范之策！

图片病毒的制作原理.....	168	一、超强免杀图片病毒揭秘 .....	171
一、什么是图片病毒 .....	168	二、图片网马实战解析 .....	174
二、图片病毒的传播方式和原理 .....	168	如何防范图片病毒.....	176
1.修改文件扩展名 .....	168	一、安装补丁 .....	176
2.寄生在压缩包中 .....	169	1.使用“自动更新” .....	176
3.利用漏洞传播 .....	169	2.使用第三方程序修补漏洞 .....	178
4.伪装成BMP图片 .....	170	3.微软网站下载单个补丁 .....	178
5.病毒程序使用图片文件图标 .....	170	二、使用图片病毒专杀工具 .....	178
图片病毒如何产生的.....	171		

### 运筹帷幄 亦正亦邪的远程控制

远程控制最早是管理员用于对远程计算机的管理和维护的一种手段，可以大大减轻工作量，提高效率；然而，随着各种远控木马的“掺合”，让远程控制变成了“强行控制”。本专题将为大家讲解常见的远程控制和远程协助实例，并介绍屏幕监控的一些具体应用。远程控制本身是一种技术手段，请大家合法使用。

## 远程控制轻松上手..... 180

### 一、最简单的远程控制UltraVNC .....180

- 1.被控端（服务器）设置 ..... 180
- 2.控制端（客户）设置 ..... 180
- 3.实现远程连接 ..... 181

### 二、维度远程控制 .....181

- 1.服务端配置 ..... 181
- 2.远程控制实战解析 ..... 182

### 三、“网络人”内网外网全拿下 .....183

- 1.用远程IP和密码快速控制 ..... 183
- 2.用会员名和自定义密码连接 ..... 185
- 3.网络人电脑控制器操控远程电脑 ..... 185

## 远程控制实例解析..... 186

### 一、WinVNC远程控制实例 .....186

- 1.Win VNC简介 ..... 186
- 2.配置服务器 ..... 186

- 3.客户端连接 ..... 186

### 二、远程控制好手PcAnywhere .....187

- 1.PcAnywhere的安装 ..... 187
- 2.PcAnywhere的基本设置 ..... 187
- 3.应用远程控制功能 ..... 188

### 三、妙用冰河陷阱防冰河 .....189

- 1.冰河陷阱简介 ..... 189
- 2.清除冰河木马 ..... 190
- 3.诱骗骇客 ..... 190

## 屏幕监控实例..... 192

### 一、E盾：另类教你玩“监控” .....192

- 1.简单配置·实现自动监控 ..... 192
- 2.查看自动监控的截图 ..... 192

### 二、屏幕间谍监控屏幕 .....193

- 1.屏幕间谍简介 ..... 193
- 2.应用实战 ..... 193

## 当心内鬼 网吧黑客攻防实例解析

由于网吧网络处于局域网环境中，所以，如果黑客要发动攻击或者监听，则享有更多的“地利”优势，这也让网吧往往成为“毒窝”。很多用户到网吧上网后发现账号被盗、游戏装备被盗，甚至网上银行也为他人买单……网吧安全急需大家重视，了解网吧黑客的攻击手段，可以更好地进行防范。

## 网吧环境的安全隐患..... 196

- 一、场景一：诱惑的链接 .....196
- 二、场景二：强大的游戏外挂 .....196
- 三、场景三：钓鱼网站 .....196
- 四、场景四：中奖信息 .....198
- 五、场景五：黑客工具 .....198
- 六、防范之策 .....198

## 网吧攻击与欺骗实例解析..... 199

### 一、当心局域网终结者的攻击 .....199

- 1.网吧攻击原理 ..... 199
- 2.局域网终结者 ..... 199

### 二、网吧ARP欺骗实例解析 .....200

- 1.欺骗原理 ..... 200
- 2.欺骗实例解析 ..... 201
- 3.ARP欺骗防范 ..... 202

### 三、网吧木马攻防实战解析 .....204

- 1.端口映射 ..... 204
- 2.挂马实战解析 ..... 205
- 3.网吧木马防范 ..... 205



### 网吧管理工具应用..... 208

#### 一、局域网监控大师 LanSee.....208

- 1. 工具简介 ..... 208
- 2. 搜索计算机 ..... 208
- 3. 搜索共享资源 ..... 208
- 4. 检查端口连接状态 ..... 208

### 二、全面封杀内网P2P: 聚生网管 .....209

- 1. 破解注册很轻松 ..... 209
- 2. 聚生网管基本配置 ..... 210
- 3. 封杀内网P2P下载 ..... 210
- 4. 限制使用聊天软件 ..... 211
- 5. 限制网络流量 ..... 211
- 6. 网络安全管理 ..... 211

## 攻守有道 网络钓鱼与网页挂马实例

网络钓鱼和网页挂马是最近几年才兴起的网络攻击方式，其主要手段就是冒充一些正规的网站来骗取用户的信任，或者干脆就在正规网站中嵌入恶意攻击代码，让访问的用户中招，轻则感染病毒木马，重则直接盗取用户的密码、骗取钱财等，对此类攻击，大家应高度重视。

### 网络钓鱼攻防实例解析..... 214

#### 一、网络防骗专家防钓鱼 .....214

- 1. 查询对方的基本个人信息 ..... 214
- 2. 文件安全性检查 ..... 214
- 3. 查询网站相关信息来判断是否为骗子 ..... 215

#### 二、简单百宝箱反钓鱼实战 .....216

- 1. 简单百宝箱如何被“钓鱼” ..... 216
- 2. 虚假钓鱼网站实例剖析 ..... 217
- 3. 两种方法检测百宝箱是否正版 ..... 217

### 网页挂马实例解析..... 218

#### 一、漏洞频曝 防范网页攻击乃当务之急...218

- 1. 浏览器安全要保证 ..... 219
- 2. 浏览器安全漏洞检测 ..... 219
- 3. 借助杀毒软件和其他安全工具 ..... 220

#### 二、静态网页挂马术 .....220

#### 三、动态网页模板挂马 .....222

#### 四、JS脚本挂马.....224

#### 五、Body和CSS挂马 .....225

### 网页挂马防范对策..... 226

#### 一、Mcafee工具深入检测网站安全 .....226

- 1. 判别网页的安全等级 ..... 226
- 2. 搜索时检测网站的安全 ..... 226
- 3. 查看站点详细信息 ..... 227

#### 二、让“巡警”为上网护驾 .....227

- 1. 加个保险箱 超级巡警账号保护神 ..... 227
- 2. 屏蔽恶意网站 畅游巡警 ..... 229

### 其它木马攻防实例解析..... 229

#### 一、影片木马攻击与防范 .....230

- 1. 木马的起源 ..... 230
- 2. 影片木马制作 ..... 230
- 3. 影片木马安全防范 ..... 233

#### 二、围剿潜藏在RMVB影片中的木马 ...235

- 1. 巧用RM恶意广告清除器..... 235
- 2. 使用快乐影音播放器清除广告 ..... 235
- 3. 迅雷也能查杀弹窗广告 ..... 236

#### 三、防不胜防，听歌也会中木马 .....236

- 1. MP3中挂木马的原理 ..... 236
- 2. 添加音乐文件 ..... 236
- 3. 设置弹窗方式和弹出时间 ..... 237
- 4. 设置木马网页地址并完成配置 ..... 237
- 5. MP3音乐“木马”防范措施 ..... 238

## 见招拆招 漏洞攻防实例解析

漏洞是指系统或软件本身存在的安全缺陷，漏洞常常被黑客利用，黑客发现系统漏洞，再配合其他手段，可以攻陷很多远程主机，威力无穷。本专题将带领大家来认识系统漏洞，并介绍常见的漏洞攻防实例和修补方法，让大家勤打补丁，封堵漏洞。

<b>Adobe Flash 漏洞攻防</b> .....	240	二、漏洞修补 .....	249
一、入侵实战解析 .....	240	<b>动画光标漏洞实例解析</b> .....	249
二、漏洞分析与防范 .....	241	一、漏洞入侵解析 .....	249
<b>IE7 0day 漏洞攻防</b> .....	241	二、安全防范 .....	250
一、漏洞简介 .....	241	<b>Serv-U 入侵防范实例</b> .....	250
二、漏洞利用代码实测 .....	242	一、准备工作 .....	250
三、木马的利用 .....	243	二、入侵实战分析 .....	251
四、漏洞的防范 .....	243	<b>博客程序 L-BLOG 攻防</b> .....	252
<b>Vista 输入法漏洞实战解析</b> .....	243	一、提权漏洞实战分析 .....	252
一、提权实战分析 .....	244	二、漏洞分析与防范 .....	255
二、安全防范 .....	247	<b>Discuz 模块编码漏洞利用</b> .....	257
<b>实战 Dcom Rpc 漏洞</b> .....	247	一、准备工作 .....	257
一、入侵解析 .....	247	二、入侵实例剖析 .....	257

## 斩断黑手 深入浅出玩转网站攻防

网站和服务器都是黑客最喜欢下手的对象，不过，由于网站和服务器都具有基本的保护措施，所以相对于一般上网的个人电脑而言显得较不易入侵成功。然而，由于很多服务器软件或操作系统的设计不良，常会造成各种各样的漏洞导致黑客们有机可乘，甚至造成网络灾难。在本专题中，将讨论黑客对网站或各类服务器的入侵及攻击流程，以及如何进行相应的防范。

<b>轻松把握网站基本知识</b> .....	260	1. 静态网页技术 .....	261
一、网站 .....	260	2. 动态网页技术 .....	261
二、常用建站技术 .....	261	3. 源代码 .....	262





4. 路径 ..... 262

## 网站常见攻击方式解密 ..... 263

- 一、入侵管理入口 ..... 263
- 二、网页木马入侵实例剖析 ..... 264
- 三、设计漏洞 ..... 266
- 四、网站安全十要素 ..... 268

## 数据库攻防实战解析 ..... 269

- 一、初级数据库下载 ..... 270
- 二、SQL Server 攻防 ..... 271
- 三、专用工具进行数据库探测 ..... 273
- 四、数据库源代码分析 ..... 274
- 五、数据库防范秘技 ..... 274

1. 本机中的数据库安全策略 ..... 274

2. 购买空间的安全策略 ..... 275

3. 特殊文件名法 ..... 276

## 服务器漏洞攻防解析 ..... 276

一、服务器安全概述 ..... 277

二、通过漏洞入侵 ..... 277

三、服务器软件问题 ..... 279

1. 设置不当 ..... 279

2. Serv-U 漏洞实战 ..... 280

3. FTP 安全防范 ..... 282

四、严格账户管理保服务器安全 ..... 283

1. 内置账户 ..... 283

2. 账户的安全配置 ..... 285