



总策划

揭秘黑客攻防手段，洞悉黑客攻防招式，成就网络安全高手

Approaches to master
入门到精通

网络安全攻防大师

15大热点专题+200个实例详解=黑客攻防大师

电脑报 ◎ 编

扫描、嗅探、网络盗号防范实例 / 加密、突破与网游攻防
病毒、木马植入与远程控制 / 网购安全与无线攻防
网吧、网站与服务器攻防



电脑报电子音像出版社
COMPUTER WORLD ELECTRONIC & AUDIO VISUAL PUBLISHING HOUSE



网络安全攻防大师

电脑报 编

内容提要



随着网络的普及,网络安全问题日益凸显。病毒、木马、黑客、钓鱼网站、挂马网页……诸如此类的安全隐患一下闯入我们的生活,这似乎不可思议,然而却实实在在地发生着。《网络安全攻防大师》针对当前复杂的网络安全环境,为大家解析黑客的各种攻击技术和攻击手段,并给出了行之有效的防范措施。具体内容包括:揭开黑客的神秘面纱、扫描与嗅探、网络盗号防范实例、加密与突破、木马植入与远程控制、网络游戏攻防、移动存储设备安全攻防、网上购物安全防范、网吧入侵与防范、图片病毒识别与解决方案、无线网络攻防、漏洞检测与修复、网站与服务器攻防、入侵安全检测等,让大家洞悉黑客招式,捍卫网络安全。



光盘要目

1. 《金山毒霸2011》
2. 黑客攻防视频教程
3. 病毒木马查杀工具
4. 账号密码保护工具
5. 黑客攻防电子书

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!

网络安全攻防大师

编 著: 电脑报

责任编辑: 李 勇

版式制作: 李品娟

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: 四川省釜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 22印张 300千字

版 号: ISBN 978-7-89476-630-4

版 次: 2011年7月第1版 2011年7月第1次印刷

定 价: 39.80元(1CD+手册)

从入门到精通 透析大师成长之路

前言

● 2001 年首度推出

● 10 年品牌、10 次再版

● 累计销量突破 100 万册

● “菜鸟”晋升“大师”的首选品牌图书

《大师禅言》系列图书自 2001 年推出以来，一直秉承《电脑报》“权威、通俗、实用”的理念，在策划、组稿、编辑等环节也一直贯穿这个理念，想读者之所想，力求让大家从一位电脑新手快速成长为电脑应用大师！事实证明，这套手册一经推出，就得到了读者的好评，多次荣登全国图书畅销排行榜，并被《中华读书报》评为“书店经理眼中的好书”，手册历经多次改版、加印，累计销量达到 100 万余册。

《大师禅言》致力于为广大读者提供最新、最热、最权威的电脑应用资讯和技巧，选取了大家非常关心的电脑组装、网络管理维护、网络安全、Excel 实战技术、Photoshop 图像处理技术等热门内容，按照由浅入深的思路进行编写：手册中既有初级入门的内容，也有中级的提高应用，最后提升到大师的独门秘笈。正文中还穿插着很多“技巧”，将电脑高手的经验和技巧毫无保留地奉献给大家，旨在让大家在成长为“大师”的坎坷道路上少走弯路。

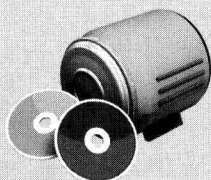
《大师禅言》携《电脑报》多年的出版经验，将电脑高手的经验整理成册，孕育了一代又一代的电脑应用高手！在广大读者强烈要求下，我们结合电脑应用的最新动态，并采纳一些读者反馈提供的宝贵意见，再次对手册进行重新策划组稿，特别推出《大师禅言》系列 2011 全新版。



电脑报

光盘内容

从入门到精通
实惠+实用+全面



分类	用途	内容
金山毒霸	查杀病毒、木马	《金山毒霸2011》永久免费软件
账号密码保护工具	保护各类账号安全	360保险箱、超级巡警账号保护神、文件密码箱、360安全卫士、可牛盗号木马专杀工具……
病毒木马查杀工具	有效防范各类病毒木马	瑞星杀毒软件、冰刃、X-scan、金山ARP防火墙、360时间保护器、360系统急救箱……
黑客攻防视频	洞悉黑客攻防，做好安全防范	防范摄像头木马、揪出隐藏在系统中的木马、开启ICP连接漏洞、清除压缩文件密码、设置远程协助、使用SuperScan……

目录

CONTENTS 网络安全攻防大师

第1章 黑客是些什么人

1.1 揭开黑客的神秘面纱	001
1.2 常见黑客攻击行为曝光	003
1.3 黑客如何利用端口	004
1.3.1 什么是计算机端口	004
1.3.2 端口的分类	004
1.3.3 开启和关闭端口	005
1.3.4 图形化的端口查看工具	006
1.4 系统进程中发现隐患	007
1.4.1 全面认识系统进程	007
1.4.2 关闭进程和重建进程	007
1.4.3 查看进程的发起程序	008
1.4.4 查看隐藏进程和远程进程	009
1.4.5 杀死病毒进程	010
1.5 常用的安全攻防术语	010
1.5.1 系统术语	010
1.5.2 网络术语	018



第2章

揭秘信息搜集、扫描与嗅探



2.1 探测操作系统版本	026
2.1.1 使用 X-scan 探测	026
2.1.2 使用 Ping 命令探测	027
2.1.3 通过网站判断	029
2.2 搜索引擎探测	030
2.2.1 搜索特殊的“关键词”	031
2.2.2 使用专用工具	031
2.3 信息的筛选	032
2.3.1 人工筛选	032
2.3.2 软件筛选	033
2.3.3 社会工程学	034
2.4 网络监听与嗅探	038
2.4.1 监听的魅力	038
2.4.2 监听实战分析	041
2.4.3 网络监听防范方法	043
2.5 扫描与嗅探实例	044
2.5.1 Sss 扫描器扫描实战	044
2.5.2 流光扫描弱口令	047
2.5.3 命令行下的嗅探器 WinDump	051

第3章

网络盗号防范实例



3.1 QQ 盗号与防范实例	054
3.1.1 当心“QQ 靓号”诱惑你	054

3.1.2 QQ 聊天记录攻防	055
3.1.3 爱 Q 大盗邮箱盗号解析	057
3.1.4 QQ 申诉也被黑客利用	059
3.1.5 识破 QQ 骗局	061
3.1.6 使用密保卡保护 QQ	065
3.2 电子邮箱攻击与防范	068
3.2.1 邮箱密码破解方式介绍	068
3.2.2 社会工程学盗取密码实例解析	068
3.2.3 邮箱使用口令的安全防范	069
3.3 网上银行安全防范	071
3.3.1 网上银行安全隐患	071
3.3.2 网上银行安全防护	072

第4章

加密、解密与安全防范



4.1 另类“隐藏”玩加密	074
4.1.1 简单几步让文件夹彻底“消失”	074
4.1.2 文件阅读后自动销毁	077
4.1.3 杀毒软件“隐藏”机密文件	080
4.2 常用密码防破解	082
4.2.1 网易闪电邮之安全隐患	082
4.2.2 当心系统密码被破解	084
4.2.3 解除 NOD32 的密码保护	085
4.2.4 揭秘破解无线路由器密码	086
4.2.5 压缩文档加密与突破	088
4.3 文件加密解密工具实战应用	092
4.3.1 图片摇身变“加密锁”	092
4.3.2 虚拟磁盘加密隐藏隐私	094
4.3.3 文件隐藏大师	096



4.3.4 电脑防删专家	098
4.3.5 军用级硬盘加密	100

第5章 木马植入与远程控制



5.1 揭秘木马攻防招式	103
5.1.1 影片木马攻防实战	103
5.1.2 巧借工具 识破木马的“马甲”	107
5.1.3 探密远程开启视频的木马	109
5.1.4 DLL 木马追踪与防范	111
5.2 网页挂马解析与防范	114
5.2.1 挂马网页识别、防治一手搞定	114
5.2.2 金山卫士双管齐下杀木马	122
5.3 远程控制实例分析	124
5.3.1 进程、屏幕轻松看	124
5.3.2 使用 PcAnywhere 远程控制	125
5.3.3 灰鸽子透过局域网远程管理	128

第6章 网络游戏攻击与防范



6.1 揭秘针对游戏的常见攻击手段	131
6.1.1 游戏存在的安全隐患	131
6.1.2 游戏外挂	133
6.1.3 游戏中暗藏木马	133
6.1.4 游戏密码保护	135
6.1.5 针对游戏的网络钓鱼	136
6.1.6 游戏中防欺诈	138

6.2 简单百宝箱反钓鱼实战	139
6.2.1 简单百宝箱如何被“钓鱼”	139
6.2.2 虚假钓鱼网站实例剖析	139
6.2.3 检测百宝箱是否正版	140
6.3 借助安全工具防范游戏攻击	141
6.3.1 可牛免费杀毒软件	141
6.3.2 防盗号就用“巨盾”	143
6.3.3 用奇虎 360 保险箱防盗号	146

第7章

移动存储设备安全攻防



7.1 初识 U 盘病毒	148
7.2 Autorun 病毒实战分析	149
7.2.1 原理与分析	150
7.2.2 病毒查找	153
7.2.3 病毒清除	153
7.2.4 故障修复	154
7.3 U 盘病毒防范之策	155
7.3.1 手工方式防 U 盘病毒	155
7.3.2 “防护盒”为 U 盘护航	157
7.3.3 内网当心 U 盘资料被窃取	159
7.3.4 为 U 盘加把“防盗锁”	160
7.3.5 USB 端口监控实战	162
7.4 USB 访问权限设置	163
7.4.1 禁止使用 USB 设备	163
7.4.2 设置可移动存储设备的权限	164



第8章

多管齐下捍卫网购安全



8.1 带毒秒杀器：当心被“秒杀”的是你	168
8.2 钓鱼网站：安能辨我是雄雌	169
8.3 团购诈骗：低价购物你不得不防	171
8.4 购物安全：网上支付选好“中介”	173
8.5 全程捍卫：金山毒霸 2011 很给力	175

第9章

网络提权与网吧攻防实例



9.1 使用代理服务器提权	177
9.1.1 获取和追踪 IP 地址	177
9.1.2 隐藏 IP 地址	179
9.1.3 使用 VPN 代理	181
9.2 巧用 Cookies 漏洞实现网站提权	185
9.2.1 Cookies 概述	185
9.2.2 查看网站写入内容	186
9.2.3 Cookies 欺骗实战	187
9.2.4 自己分析 Cookies 漏洞	189
9.3 网吧攻防实例剖析	192
9.3.1 剖析网吧安全环境	192
9.3.2 突破网吧限制	195
9.3.3 网吧常见攻击与防范	198
9.3.4 溢出拿网吧主机	199
9.3.5 网吧安全防范	201

第10章**图片病毒识别与防治方案**

10.1 图片病毒的制作原理	203
10.1.1 什么是图片病毒	203
10.1.2 图片病毒的传播方式和原理	204
10.2 图片病毒如何产生的	206
10.2.1 超强免杀图片病毒揭秘	207
10.2.2 图片网马实战解析	210
10.3 如何防范图片病毒	212
10.3.1 安装补丁	212
10.3.2 安装杀毒软件	214
10.3.3 使用图片病毒专杀工具	215

第11章**无线网络破解与安全防范**

11.1 无线网络的安全隐患	216
11.1.1 信号被盗：“一家掏钱多家用”	216
11.1.2 防范会议大厅数据被盗用	217
11.1.3 在无线局域网中“隐身”	218
11.1.4 禁止部分人上网	218
11.2 无线 WEP 加密破解与防范	219
11.2.1 无线 WEP 加密方法	219
11.2.2 轻松获取 WEP 密码	219
11.2.3 当心无线 WEP 被破解	220
11.2.4 防范方法	223



11.3 WPA 加密破解与防范	224
11.3.1 WPA、WEP 无线加密对比	224
11.3.2 WPA 加密被破解后的防范	225
11.4 消除无线安全隐患的 8 种手段	226

第12章

常见漏洞攻防实例剖析



12.1 通通透透认识系统漏洞	229
12.1.1 什么是系统漏洞	229
12.1.2 轻松配置 自动更新补丁	229
12.1.3 轻松备份补丁文件	230
12.1.4 用金山装机精灵快速打补丁	231
12.2 上网就躲不过：IE7 0day 漏洞攻防	232
12.2.1 漏洞简介	232
12.2.2 漏洞利用代码实测	233
12.2.3 木马利用剖析	233
12.2.4 IE7 0day 漏洞的防范	234
12.3 Word 0day 漏洞攻防解析	234
12.3.1 漏洞简介	234
12.3.2 攻击实例解析	235
12.3.3 安全防范	236
12.4 别被美丽蒙骗：Adobe Flash 漏洞攻防	237
12.4.1 入侵解析	237
12.4.2 漏洞分析与防范	238
12.5 零距离接触 Vista 输入法漏洞	238
12.5.1 提权实战	239
12.5.2 安全防范	242

12.6 缓冲区溢出：实战 Dcom Rpc 漏洞	242
12.6.1 入侵实战解析	242
12.6.2 漏洞修补	244
12.7 远程攻击你：动画光标漏洞	244
12.7.1 漏洞入侵实战	244
12.7.2 安全防范	245
12.8 FTP 安全隐患：Serv-U 入侵攻防	245
12.8.1 准备工作	245
12.8.2 入侵实战	246
12.9 论坛也遭殃：动网程序入侵	247
12.9.1 入侵实例分析	247
12.9.2 上传漏洞防范	249

第13章

网站攻防实例分析



13.1 网站安全初识	250
13.1.1 网站安全现状	250
13.1.2 网站攻击概述	251
13.1.3 网站语言	252
13.2 登录口令攻防	253
13.2.1 源代码分析破解	253
13.2.2 使用软件破解	256
13.2.3 使用注入破解	257
13.3 “一句话木马”攻防	258
13.3.1 木马概述	258
13.3.2 入侵实战	259
13.3.3 安全防范	261



13.4 网站漏洞攻防	262
13.4.1 漏洞简介与防范策略	262
13.4.2 批量入侵实战	262
13.5 网站数据库攻防	264
13.5.1 巧妙利用 500 错误入侵	264
13.5.2 利用关键字下载数据库	266
13.5.3 使用 NBSI 入侵	266
13.5.4 源代码分析	267
13.5.5 数据库防范秘技	268

第14章

服务器攻防与安全配置



14.1 服务器安全概述	270
14.1.1 什么是服务器	270
14.1.2 服务器入侵渠道	271
14.2 实战 CC 攻击	272
14.2.1 攻击原理	272
14.2.2 攻击实例分析	273
14.2.3 识别 CC 攻击	275
14.2.4 轻松抵御 CC 攻击	275
14.3 DDoS 攻击实战剖析	278
14.3.1 DDoS 攻击原理	278
14.3.2 攻击实例	278
14.3.3 识别 DDoS 攻击	279
14.3.4 DDoS 防范与反击	280
14.4 服务器漏洞攻防	282
14.4.1 攻击原理	282
14.4.2 攻击实例	283
14.4.3 安全防范	285

14.5 数据库攻防	286
14.5.1 数据库概述	286
14.5.2 攻击实例之 SQL 溢出	287
14.5.3 实例攻击之 SQL 弱口令	289
14.5.4 实例攻击之 SQL 2005 注入	290
14.6 服务器安全配置	290
14.6.1 安装补丁	291
14.6.2 杀毒软件	292
14.6.3 权限设置	294
14.6.4 删除 LAN 设置	294

第15章

入侵检测与日志管理



15.1 什么是入侵检测	297
15.2 用 X-Scan 检测目标主机	301
15.3 用 IIS Lock Tool 扫描服务器	302
15.4 防患于未然	305
15.5 让日志成为安全管理好助手	309
15.5.1 日志概述	309
15.5.2 安全日志的启用	312
15.5.3 四项基本技能	314
15.5.4 清除与保存日志	315
15.5.5 远程管理日志	317
15.6 自己动手检测启动项安全隐患	318
15.6.1 他们是如何搞破坏的	318
15.6.2 黑客会怎么做	320
15.6.3 禁止恶意启动项运行	324



附录

揭秘黑客高手的神来之笔：批处理



一、初识批处理	328
1. 创建批处理文件	328
2. 基本命令	330
3. 参数	332
二、批处理实例精华	333
1. 批量检测入机存活	333
2. 检查是否感染 Wollf 木马	333
3. 操作注册表	334
4. 终止进程	334
5. 遍历磁盘并删除 gho 文件	335
6. 禁止网络共享	335
7. 获取当前计算机的 IP 和 MAC 地址	336
8. 磁盘映射	336