



披露黑客练功全过程
识破黑客入侵小伎俩
轻松实现从菜鸟到大虾
练就黑客终极必杀技

矛与盾



36个知识点多媒体视频讲解
让你快速从入门到精通

黑客攻防与脚本编程

武新华 陈艳艳 王英英 等编著



机械工业出版社
China Machine Press

TP393.08
W986-7

-04

矛与盾

黑客攻防与脚本编程

TP393.08

W986-7

武新华 陈艳艳 王英英 等编著



机械工业出版社
China Machine Press

本书对每一个入侵步骤作详细的分析,以推断入侵者在每一个入侵步骤的目的以及所要完成的任务,并对入侵过程中常见问题作必要的说明与解答。全书共分为 13 章,主要包括黑客入门知识基础、黑客的攻击方式、Windows 系统编程与网站脚本、后门程序编程基础、高级系统后门编程技术、黑客程序的配置和数据包嗅探、编程攻击与防御实例、SQL 注入攻击与防范技术、数据库入侵与防范技术、Cookies 攻击与防范技术、网络上传漏洞的攻击与防范、恶意脚本入侵与防御、数据备份升级与恢复等内容。

本书内容丰富全面,图文并茂,深入浅出,面向广大网络爱好者,也适用于网络安全从业人员及网络管理者,同时可作为一本速查手册。

版权所有,侵权必究

本书法律顾问 北京市展达律师事务所

图书在版编目(CIP)数据

矛与盾——黑客攻防与脚本编程 / 武新华等编著. —北京:机械工业出版社, 2010.1

ISBN 978-7-111-28574-8

I. 矛… II. 武… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2009)第 188878 号

机械工业出版社(北京市西城区百万庄大街 22 号 邮政编码 100037)

责任编辑:李东震

北京京师印务有限公司印刷

2010 年 1 月第 1 版第 1 次印刷

184mm×260mm·22.5 印张

标准书号:ISBN 978-7-111-28574-8

ISBN 978-7-89451-258-1(光盘)

定价:48.00 元(附光盘)

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

客服热线:(010) 88378991; 88361066

购书热线:(010) 68326294; 88379649; 68995259

投稿热线:(010) 88379604

读者信箱:hzjsj@hzbook.com

前言

本书本着防患于未然的主旨，着重而详细地介绍了各种黑客入侵网页的手段，概括绝大部分的攻击方式。本书虽然详细解说了每个攻击手法的原理与实际操作，但毕竟如何防范这些入侵才是本书的重点。想要开发安全的 PHP 应用程序，就赶快拿起这本书仔细地阅读吧！只有使读者在了解黑客攻击知识的基础上，能够最大限度地做到“知己知彼”，才有可能在遭受黑客攻击时尽量减少自己的损失。

下面简要介绍本书的特点、学习方法以及提供的服务。

本书内容

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以最浅显易懂的语言，介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具。本书内容主要包括：黑客入门知识基础、黑客的攻击方式、Windows 系统编程与网站脚本、后门程序编程基础、高级系统后门编程技术、黑客程序的配置和数据包嗅探、编程攻击与防御实例、SQL 注入攻击与防范技术、数据库入侵与防范技术、Cookies 攻击与防范技术、网络上传漏洞的攻击与防范、恶意脚本入侵与防御、数据备份升级与恢复等内容。本书详细地讲述了防护黑客攻击的方法及黑客的攻击与防范技术，使读者在实际应用中碰到黑客攻击时，能够做到“胸有成竹”。

读者运用本书介绍的黑客攻击防守方法去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

本书几个具体网站例子，已经将具体信息提交给网站进行了修改。

增值服务

本书附赠的光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过增加读者对主流操作手法感性认识的方式，使读者实现高效学习。

此外，如发现本书中有需要改进之处，还可通过访问 <http://www.newtop01.com> 或 QQ: 274648972 与编者进行沟通，编者将衷心感谢提供建议的读者，并真心希望和广大读者互动的过程中能得到提高。

组织方式

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网络入侵与防御的全过程。

- 真正的以图来解释每一个知识点及操作实例，基础知识讲解、范例与练习结合，学习周期最短，阅读最轻松。



- ❑ 作者采用最为通俗易懂的图文解说,“理论+实战 图文+视频=让读者快速入门”,即使是电脑新手也能通读全书。
- ❑ 用任务驱动、情景教学的方式来介绍,在学习案例过程中可掌握知识点,学习目的性、指向性最强。最新黑客技术盘点,让读者实现“先下手为强”。

本书特色

本书以情景教学、案例驱动及任务进阶为鲜明特色,在书中可以看到一个个生动的情景案例。通过完成一个个实践任务,读者可以轻松掌握各种知识点,在不知不觉中快速提升实战技能。

- ❑ 技术最新:当前最新技术,热点技术,常用相关工具软件都在本书有所涉及,有关黑客攻防技术、方法与思路,也做了重要讲解,并通过实例介绍综合技术的运用手段。
- ❑ 高效模式:完全站在实用角度介绍黑客攻防技术,突出了实用性和案例分析,全程图解模式可彻底克服攻防操作的学习障碍,学习起来省时、省力,易于上手。
- ❑ 内容合理:结合图解,标注和多媒体教学,精选入门读者最迫切需要掌握的知识点,构建一个实用、够用、完整的知识体系。
- ❑ 举一反三:详细分析每一个操作案例,力求通过一个知识点的讲解,以实现读者用更少时间尽快掌握黑客编程技术,让读者彻底理解和掌握类似场合的应对思路。

读者对象

本书作为一本面向广大网络爱好者的速查手册,适合如下读者学习使用:

- ❑ 电脑爱好者、提高者;
- ❑ 具备一定黑客知识基础和工具使用基础的读者;
- ❑ 网络管理人员;
- ❑ 喜欢研究黑客防御技术的网友;
- ❑ 大中专院校相关专业学生。

本书作者

本书作者团队长期从事网络安全管理工作,都具有较强的实践操作能力及一线拼杀经验,可带领广大醉心技术者穿越迷雾,把黑客们的伎俩看清楚。参与本书编写工作的有:冯世雄负责第1章,张晓新负责第2章,陈艳艳、李防负责第3、4、5、6章,王肖苗负责第7章,孙世宁负责第8章,杨平负责第9章,段玲华负责第10章,李伟负责第11章,王英英负责第12章,郑静负责第13章,最后由武新华通审全稿。我们虽满腔热情,但限于自己的水平,书中仍难免有疏漏之处,因此,还望读者本着共同探讨、共同进步的平和心态来阅读本书。作者心存谨敬,随时恭候您提出的宝贵意见。

最后,需要提醒大家的是:根据国家有关法律规定,任何利用黑客技术攻击他人的行为都属于违法行为,希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人进行攻击,否则后果自负,切记切记!

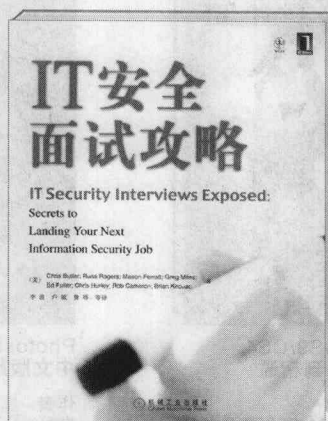
编者

2009年11月8日

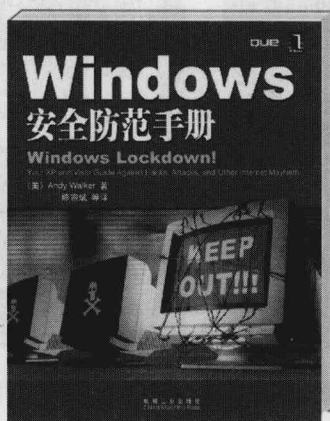
好书推荐



作者: Pedram Amini
书号: 978-7-111-25755-4
定价: 59.00元



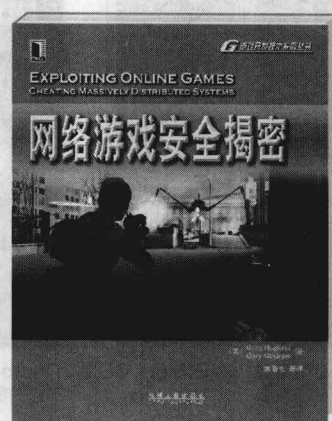
作者: Chris Butler 等
书号: 978-7-111-25507-9
定价: 29.00元



作者: Andy Walker
书号: 978-7-111-26519-1
定价: 49.00元

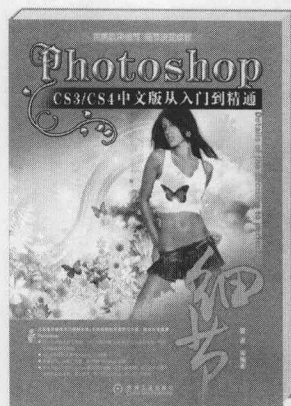


作者: David Rice
书号: 978-7-111-25229-0
定价: 39.00元



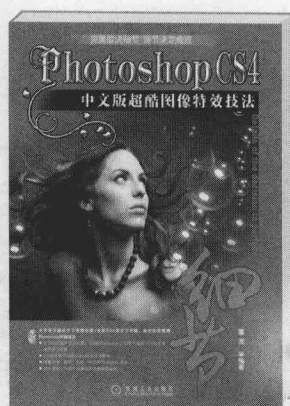
作者: Greg Hoglund 等
书号: 978-7-111-25522-2
定价: 45.00元

好书推荐



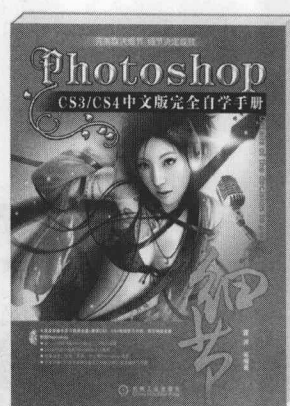
**Photoshop CS3/CS4
中文版从入门到精通**

作者：雷波
书号：978-7-111-26093-6
定价：89.00元



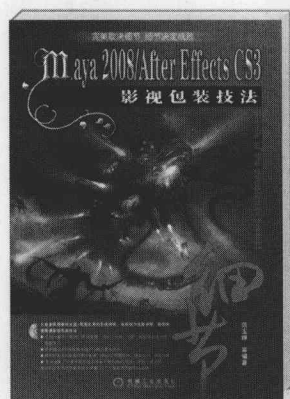
**Photoshop CS4
中文版超酷图像特效技法**

作者：雷剑
书号：978-7-111-26106-3
定价：79.80元



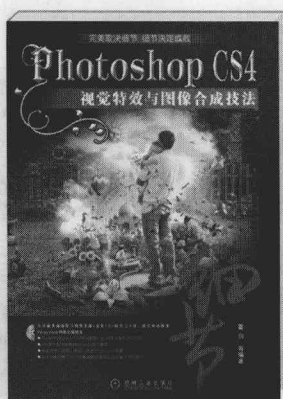
**Photoshop CS3/CS4
中文版完全自学手册**

作者：雷剑
书号：978-7-111-26092-9
定价：79.00元



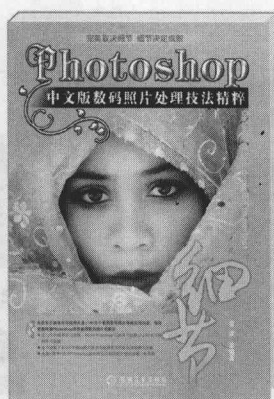
**Maya 2008/After Effects CS3
影视包装技法**

作者：范玉婵
书号：978-7-111-26105-6
定价：88.00元



**Photoshop CS4
视觉特效与图像合成技法**

作者：雷剑
书号：978-7-111-26094-3
定价：79.00元



**Photoshop
中文版数码照片处理技法精粹**

作者：雷波
书号：978-7-111-24411-0
定价：69.80元



**3ds max/VRay
室内效果图渲染技法**

作者：范玉婵
书号：978-7-111-26135-3
定价：79.00元

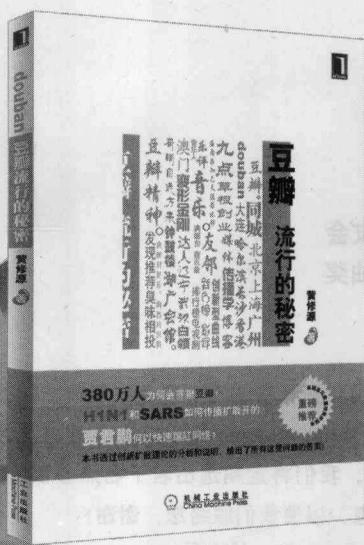
中国IT励志小说

一个月重印三次

让无数企业高管、IT开发者、创业者、高校学生
彻夜啃读叹为观止！

作者是一位《华尔街杂志》的著名记者，文笔犀利，用词泼辣，豪放不羁，微软NT团队的几十个人物，在作者的笔下栩栩如生，作者直言不讳写出他们的缺点，甚至于相貌、家庭、婚恋、事业，大卫·卡特勒是其中的灵魂人物，他是一位计算机的天才，汇编高手，但他的性格很暴躁，脾气倔犟，这也许就是我们传说中的鬼才吧，在昨天刚拿到书时，我并没有立即去看这本书，随手放在了桌边，晚上躺在床上顺手翻了一下，结果一发不可收拾，一直看到早晨5点多才睡觉，要不是顾及今天上班，估计我还会继续看下去。有人说在本书中仅看对卡特勒的描述就很值了，建议大家有空时也读读这本书，看看那些个性鲜明的人物他们的传奇故事，也许我们应该从中学到点什么。

——博客园知名博主 李会军



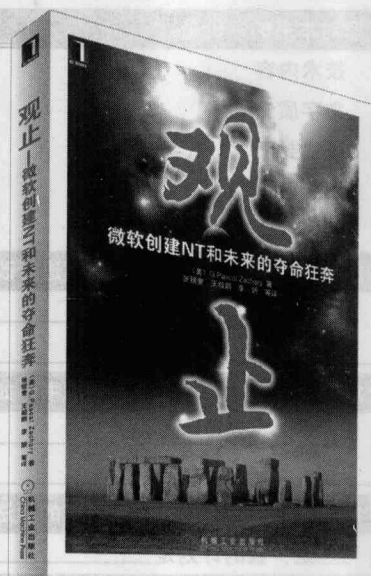
《豆瓣，流行的秘密》 ——传递爱和理想 一本正在漂流的图书

当你在KFC、麦当劳、星巴克甚至在地铁站里发现一本《豆瓣，流行的秘密》时，不要以为这是一本被丢弃的图书，请把它拣起来，这是一本正在全国漂流的图书，这本漂流的图书，它传播的不仅是一位年轻创业者的理想，也传承着一种阅读的文化。

看了这本书，也许不能让你的产品或网站突然流行起来，但至少，它能让你知道你的产品或网站为什么没能流行起来。下一次，也许你也能创造出一个大流行。

如果你想了解为什么很多网站吸引客户的秘诀，如果你想知道为什么长尾理论只会在互联网的产品中出现，那么我推荐你阅读这本书籍。它很短小，语言简单，例子很实际，它希望用简单的语言告诉你一件我已经发现的或许你还不知道的秘密，你可以在闲暇的周末泡杯咖啡，一边慢慢喝一边阅读它，我想这会是一个很充实的周末。

作者黄修源，正在和他的团队一起在实践中很多书中所说的理论，番茄树正是他们正在运营的网站。2个月的时间从ALEXA的100多万名到24000名，没有花一分钱广告费，“其实我们只是在实践我写的书中的一些有意思的理论而已！”修源这样说。



“在微软的成长过程中，一直伴随着对梦想的不懈追求。本书展现了微软的天才团队追梦过程里的精彩片断——他们付出了艰苦卓绝的努力，经历了犹疑、冲突和痛苦，但他们的成就今天仍然在影响世界。”

——微软全球副总裁 张亚勤



专业成就人生
立体服务大众

www.hzbook.com

填写读者调查表 加入华章书友会
获赠精彩技术书 参与活动和抽奖

尊敬的读者：

感谢您选择华章图书。为了聆听您的意见，以便我们能够为您提供更优秀的图书产品，敬请您抽出宝贵的时间填写本表，并按底部的地址邮寄给我们（您也可通过www.hzbook.com填写本表）。您将加入我们的“华章书友会”，及时获得新书资讯，免费参加书友会活动。我们将定期选出若干名热心读者，免费赠送我们出版的图书。请一定填写书名书号并留全您的联系信息，以便我们联络您，谢谢！

书名：

书号：7-111-()

姓名：	性别： ☐ 男 ☐ 女	年龄：	职业：
通信地址：		E-mail：	
电话：	手机：	邮编：	

1. 您是如何获知本书的：

☐ 朋友推荐 ☐ 书店 ☐ 图书目录 ☐ 杂志、报纸、网络等 ☐ 其他

2. 您从哪里购买本书：

☐ 新华书店 ☐ 计算机专业书店 ☐ 网上书店 ☐ 其他

3. 您对本书的评价是：

技术内容	☐ 很好	☐ 一般	☐ 较差	☐ 理由_____
文字质量	☐ 很好	☐ 一般	☐ 较差	☐ 理由_____
版式封面	☐ 很好	☐ 一般	☐ 较差	☐ 理由_____
印装质量	☐ 很好	☐ 一般	☐ 较差	☐ 理由_____
图书定价	☐ 太高	☐ 合适	☐ 较低	☐ 理由_____

4. 您希望我们的图书在哪些方面进行改进？

5. 您最希望我们出版哪方面的图书？如果有英文版请写出书名。

6. 您有没有写作或翻译技术图书的想法？

☐ 是，我的计划是_____ ☐ 否

7. 您希望获取图书信息的形式：

☐ 邮件 ☐ 信函 ☐ 短信 ☐ 其他_____

请寄：北京市西城区百万庄南街1号 机械工业出版社 华章公司 计算机图书策划部收
邮编：100037 电话：(010) 88379512 传真：(010) 68311602 E-mail: hzsj@hzbook.com

目 录

前言

第1章 黑客攻防知识	1
1.1 黑客基础知识	2
1.1.1 进程、端口和服务	2
1.1.2 文件和文件系统概述	5
1.1.3 DOS 系统常用的命令	5
1.1.4 Windows 注册表	12
1.2 常见的网络协议	13
1.2.1 TCP/IP	13
1.2.2 IP	13
1.2.3 ARP	14
1.2.4 ICMP	15
1.3 创建安全测试环境	16
1.3.1 安全测试环境概述	16
1.3.2 虚拟机软件概述	16
1.3.3 用 VMware 创建虚拟环境	17
1.3.4 安装虚拟工具	24
1.3.5 在虚拟机上假设 IIS 服务器	25
1.3.6 在虚拟机中安装网站	28
1.4 必要的黑客攻防知识	29
1.4.1 常见的黑客攻击流程	29
1.4.2 常用的网络防御技术	30
1.5 专家点拨	31
1.6 总结与经验积累	32
第2章 剖析黑客的攻击方式	33
2.1 网络欺骗攻击	34
2.1.1 攻击原理	34
2.1.2 攻击与防御实战	36
2.2 口令猜解攻击	38
2.2.1 攻击原理	38
2.2.2 攻击与防御实战	40
2.3 缓冲区溢出攻击	46
2.3.1 攻击原理	46
2.3.2 攻击与防御实战	49



2.4 专家点拨	54
2.5 总结与经验积累	54
第3章 Windows 系统编程与网站脚本	55
3.1 黑客编程简介	56
3.1.1 黑客编程语言介绍	56
3.1.2 黑客与编程	57
3.2 Windows 系统编程概述	57
3.2.1 网络通信编程简介	58
3.2.2 文件操作编程简介	64
3.2.3 注册表编程简介	67
3.2.4 进程和线程编程简介	70
3.3 网站脚本入侵与防范	76
3.3.1 Web 脚本攻击概述	77
3.3.2 脚本漏洞的根源与防范	78
3.4 专家点拨	79
3.5 总结与经验积累	79
第4章 后门程序编程基础	80
4.1 后门概述	81
4.2 编写简单的 cmdshell 程序	82
4.2.1 管道通信技术简介	82
4.2.2 正向连接后门的编程	85
4.2.3 反向连接后门的编程	91
4.3 编写简单的后门程序	92
4.3.1 编程实现远程终端的开启	92
4.3.2 编程实现文件查找功能	95
4.3.3 编程实现重启、关机和注销	100
4.3.4 编程实现 http 下载文件	103
4.3.5 编程实现 cmdshell 和各功能的切换	105
4.4 实现自启动功能的编程技术	107
4.4.1 注册表自启动的实现	107
4.4.2 ActiveX 自启动的实现	109
4.4.3 系统服务自启动的实现	111
4.4.4 svchost.exe 自动加载启动的实现	119
4.5 专家点拨	120
4.6 总结与经验积累	120
第5章 高级系统后门编程技术	121
5.1 远程线程技术	122
5.1.1 初步的远程线程注入技术	122
5.1.2 编写远程线程注入后门	126
5.1.3 远程线程技术的发展	127
5.2 端口复用后门	130



5.2.1 后门思路	130
5.2.2 具体编程实现	130
5.3 专家点拨	134
5.4 总结与经验积累	134
第6章 黑客程序的配置和数据包嗅探	135
6.1 文件生成技术	136
6.1.1 资源法生成文件	136
6.1.2 附加文件法生成文件	140
6.2 黑客程序的配置	143
6.2.1 数据替换法	143
6.2.2 附加信息法	149
6.3 数据包嗅探	151
6.3.1 原始套接字基础	151
6.3.2 利用 ICMP 原始套接字实现 ping 程序	152
6.3.3 基于原始套接字的嗅探技术	156
6.3.4 利用 Packet32 实现 ARP 攻击	161
6.4 如何防御黑客进行嗅探	170
6.5 专家点拨	171
6.6 总结与经验积累	171
第7章 编程攻击与防御实例	172
7.1 通过程序创建木马攻防实战	173
7.1.1 VB 木马编写与防范	173
7.1.2 基于 ICMP 的 VC 木马编写	178
7.1.3 基于 Delphi 的木马编写	181
7.1.4 电子眼——计算机扫描技术的编程	184
7.2 隐藏防复制程序的运行	187
7.3 专家点拨	189
7.4 总结与经验积累	189
第8章 SQL 注入攻击与防范技术	190
8.1 SQL 注入攻击前的准备	191
8.1.1 攻击前的准备	191
8.1.2 寻找攻击入口	193
8.1.3 判断 SQL 注入点类型	194
8.1.4 判断目标数据库类型	195
8.2 常见的注入工具	196
8.2.1 NBSI 注入工具	196
8.2.2 啊 D 注入工具	199
8.2.3 Domain 注入工具	201
8.2.4 ZBSI 注入工具	204
8.3 'or' = 'or' 经典漏洞攻击	205
8.3.1 'or' = 'or' 攻击突破登录验证	205



8.3.2 未过滤的 request.form 造成的注入	206
8.4 缺失单引号与空格的引入	210
8.4.1 转换编码, 绕过程序过滤	210
8.4.2 /**/替换空格的注入攻击	212
8.4.3 具体的防范措施	220
8.5 Update 注入攻击	220
8.6 SQL 注入攻击的防范	223
8.7 专家点拨	226
8.8 总结与经验积累	226
第9章 数据库入侵与防范技术	227
9.1 常见数据库漏洞简介	228
9.1.1 数据库下载漏洞	228
9.1.2 暴库漏洞	228
9.2 数据库连接的基础知识	229
9.2.1 ASP 与 ADO 模块	229
9.2.2 ADO 对象存取数据库	230
9.2.3 数据库连接代码	231
9.3 默认数据库下载漏洞的攻击	231
9.3.1 论坛网站的基本搭建流程	231
9.3.2 数据库下载漏洞的攻击流程	232
9.3.3 下载网站的数据库	234
9.3.4 数据库下载漏洞的防范	235
9.4 利用 Google 搜索网站漏洞	236
9.4.1 利用 Google 搜索网站信息	237
9.4.2 Google 暴库漏洞的分析与防范	238
9.5 暴库漏洞攻击实例	239
9.5.1 conn.asp 暴库法	239
9.5.2 %5c 暴库法	240
9.5.3 防御暴库攻击	242
9.6 专家点拨	243
9.7 总结与经验积累	244
第10章 Cookies 攻击与防范技术	245
10.1 Cookies 欺骗攻击实例	246
10.1.1 Cookies 信息的安全隐患	246
10.1.2 利用 IECookiesView 获得目标计算机中的 Cookies 信息	247
10.1.3 利用 Cookies 欺骗漏洞掌握网站	248
10.2 深入探讨 Cookies 欺骗漏洞	251
10.2.1 数据库与 Cookies 的关系	252
10.2.2 Cookies 欺骗与上传攻击	254
10.2.3 ClassID 的欺骗入侵	258
10.2.4 用户名的欺骗入侵	259



10.3 Cookies 欺骗的防范措施	260
10.4 专家点拨	262
10.5 总结与经验积累	262
第 11 章 网络上传漏洞的攻击与防范	263
11.1 多余映射与上传攻击	264
11.1.1 文件上传漏洞的基本原理	264
11.1.2 asp.dll 映射的攻击	264
11.1.3 stm 与 shtml 的映射攻击	269
11.2 点与 Windows 命名机制的漏洞	272
11.2.1 Windows 命名机制与程序漏洞	272
11.2.2 变换文件名产生的漏洞	274
11.3 二次循环产生的漏洞	278
11.3.1 MyPower 上传攻击测试	278
11.3.2 本地提交上传流程	281
11.3.3 二次上传产生的逻辑错误	283
11.3.4 沁竹音乐网上传漏洞攻击	284
11.3.5 桃源多功能留言板上传漏洞攻击	287
11.4 利用 Winsock Expert 进行上传攻击	288
11.4.1 Winsock Expert 与上传漏洞攻击	288
11.4.2 Winsock Expert 与 NC 结合攻破天意商务网	290
11.5 不受控制的上传攻击	295
11.6 专家点拨	297
11.7 总结与经验积累	298
第 12 章 恶意脚本入侵与防御	299
12.1 恶意脚本论坛入侵与防御	300
12.1.1 极易入侵的 BBS3000 论坛	300
12.1.2 并不安全的论坛点歌台漏洞	302
12.1.3 雷奥论坛 LB5000 也存在着漏洞	303
12.1.4 被种上木马的 DV7.0 上传漏洞	307
12.2 剖析恶意脚本的巧妙运用	309
12.2.1 全面提升 ASP 木马权限	309
12.2.2 利用恶意代码获得用户的 Cookies	310
12.2.3 在动网论坛中嵌入网页木马	311
12.2.4 利用恶意脚本实现 Cookies 注入攻击	313
12.3 恶意脚本入侵的防御	314
12.4 专家点拨	315
12.5 总结与经验积累	316
第 13 章 数据备份升级与恢复	317
13.1 全面了解备份升级	318
13.1.1 数据备份概述	318
13.1.2 系统的补丁升级	319



13.1.3 实现备份操作	320
13.2 对常用的数据进行备份和还原	324
13.2.1 对操作系统进行备份和还原	324
13.2.2 备份/还原注册表	328
13.2.3 备份/还原 IE 收藏夹	329
13.2.4 备份/还原驱动程序	332
13.2.5 备份/还原病毒库	334
13.2.6 备份/还原数据库	336
13.3 全面了解数据恢复	338
13.3.1 数据恢复概述	338
13.3.2 造成数据丢失的原因	338
13.3.3 使用和维护硬盘的注意事项	339
13.4 强大的数据恢复工具	340
13.4.1 EasyRecovery 使用详解	340
13.4.2 FinalData 使用详解	344
13.5 专家点拨	346
13.6 总结与经验积累	346



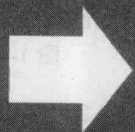
矛与盾——黑客攻防与脚本编程

①

第 1 章 黑客攻防知识

重点提示

- ⊗ 黑客基础知识
- ⊗ 常见的网络协议
- ⊗ 创建安全测试环境





随着互联网对人们日常生活影响的深入，网络的安全问题也引起了人们高度关注。而黑客则是网络世界中很神秘的一类人，他们有时会义务去维护网络的安全，有时却又以网络破坏者的形象出现。

1.1 黑客基础知识

要成为一名合格的黑客，就必须对操作系统相关的知识有充分地了解，包括进程、端口、服务、文件、文件系统、常用的 DOS 命令和注册表等。只有充分了解了这些知识，才可以提高攻击的成功几率。

1.1.1 进程、端口和服务

一般情况下，计算机中的进程、端口和服务都会给黑客可趁之机，所以在深入了解黑客常用的攻击手段之前，有必要对他们使用的相关基础知识有初步的了解。

1. 进程

进程是一个正在执行的程序。运行一个程序，就启动了一个进程。程序是静态的，进程是动态的。进程可以分为系统进程和用户进程两种。凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。进程是操作系统进行资源分配的单位。

在 Windows 系统中按“Ctrl+Alt+Delete”组合键，即可打开【任务管理器】窗口。切换到“进程”选项卡，即可看到本机中开启的进程，如图 1-1 所示。如果想设置进程显示的内容，则选择【查看】→【选择列】菜单项，在【选择列】对话框中勾选相应的复选框，如图 1-2 所示。

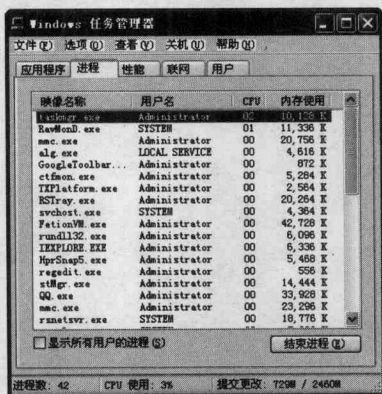


图 1-1 查看本机中开启的进程

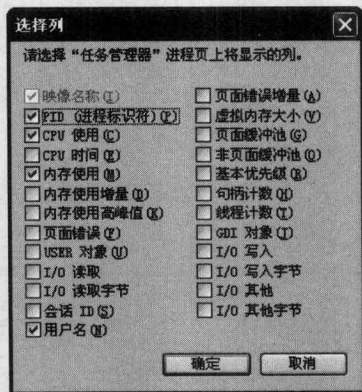


图 1-2 【选择列】对话框

2. 端口

计算机“端口”是计算机与外界通信的出入口。其中硬件领域的端口又称接口，如 USB 端口、串行端口等；而软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，包括一些数据结构和 I/O（基本输入/输出）缓冲区。

在网络技术中，端口有两种含义：一是物理意义上的端口，如集线器、交换机、路由器等