

1CD 多媒体教学光盘

附赠 40段视频教程，时间长达150分钟
(系统安装·重装·备份与还原)、(电脑上网)
(电脑组装·维护与故障排除) 教学视频



电脑安全 与黑客攻防

前沿文化/编著

从新手到高手



内容**全面**实用
讲解**清晰**易懂



彩色图书



视频光盘



超值附赠

资深电脑安全专家编写，让您**简单快捷**地学会各种工具与技巧，今后**轻松**地保护数据与隐私



科学出版社

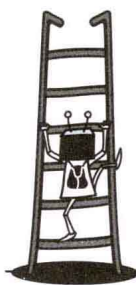


电脑安全

与黑客攻防

前沿文化/编著

从新手到高手



科学出版社

内 容 简 介

本书针对初学者的需求,全面、详细地讲解了电脑安全保障与黑客攻防的基本方法、疑难问题与相关技巧。图书在讲解上图文并茂,重视操作技巧的传授,并在图片中清晰地标注出要进行操作的位置与操作内容,并对重点、难点操作均配有视频教程,以求您能高效、完整地掌握本书内容。

本书共分为 16 章,包括网络安全初接触、了解随处可见的计算机病毒、揭开黑客与木马的面纱、掌握 Windows 系统的漏洞和防范妙招、黑客常用命令详解、搜集远程计算机的信息、远程入侵计算机、木马入侵与防御、QQ 攻击与防御、电子邮箱攻击与防御、来自网页的攻击与防御方法、防范扫描与恶意软件、网站攻防入门、网站上传漏洞的攻击和防御、网站脚本注入的攻击与防御等内容。

本书既可供想要学习电脑安全保障与黑客攻防的用户使用,同时也可以作为电脑培训班的培训教材或学习辅导书。

图书在版编目(CIP)数据

电脑安全与黑客攻防从新手到高手/前沿文化编著.

—北京:科学出版社,2012.5

ISBN 978-7-03-034078-8

I. ①电… II. ①前… III. ①电子计算机—安全技术
②计算机网络—安全技术 IV. ①TP309

中国版本图书馆 CIP 数据核字(2012)第 073787 号

责任编辑:周 勤 吴俊华 / 责任校对:杨慧芳

责任印刷:华 程 / 封面设计:彭 彭

科学出版社 出版

北京东黄城根北街 16 号

邮政编码:100717

<http://www.sciencep.com>

中国科技出版传媒集团新世纪书局策划

北京朝阳新艺印刷有限公司印刷

中国科技出版传媒集团新世纪书局发行 各地新华书店经销

*

2012 年 6 月第 一 版 开本:16 开

2012 年 6 月第一次印刷 印张:20.25

字数:443 000

定价:45.00 元(含 1CD 价格)

(如有印装质量问题,我社负责调换)

新华书店
PDG

PREFACE

前言

如今电脑和网络已经深入人们的日常生活，在办公、学习和娱乐等多个领域发挥着重要作用，极大地改变了人们长久以来形成的传统思维和生活方式。然而与此同时，电脑和网络的安全问题也变得日益严重，各种病毒、木马和黑客攻击层出不穷，其手法更是不断变化，严重威胁着人们的电脑安全，给人们的日常工作和生活带来了极大的麻烦，已引起人们的高度重视。本书从电脑安全和黑客攻防的基础知识和基本操作入手，结合大量实例，采用知识点讲解与动手练习相结合的方式，详细介绍了电脑安全的保障方法和黑客攻击的防范技巧。

本书内容系统、全面，充分考虑电脑用户的实际情况，将电脑安全保障的理论与实践相融合，为读者解析黑客攻防的各种技术、手段以及相应的防范措施，力求使您快速掌握电脑安全防范的思路与方法，轻松保障电脑的使用安全。全书采用图片配合文字说明的方式对知识点进行讲解，步骤清晰、完备，保证您轻松、顺利地学会。在介绍黑客攻防实例时，尽量选用常见的、典型的案例，以便于读者能举一反三，快速应用于实践。

本书共分为16章，包括网络安全初接触、了解随处可见的计算机病毒、揭开黑客与木马的面纱、掌握Windows系统的漏洞和防范妙招、黑客常用命令详解、搜集远程计算机的信息、远程入侵计算机、木马入侵与防御、QQ攻击与防御、电子邮箱攻击与防御、来自网页的攻击与防御方法、防范扫描与恶意软件、网站攻防入门、网站上传漏洞的攻击和防御、网站脚本注入的攻击与防御等内容。

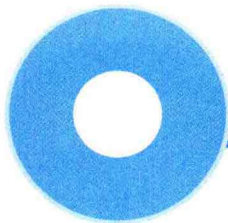
本书配1张多媒体教学CD光盘，包含了40个重点操作实例的视频教学录像，播放时间长达150分钟。此外，为了让您能够掌握更多的知识，特贴心赠送畅销图书《电脑上网》、《电脑组装、维护与故障排除》和《系统安装、重装、备份与还原》的视频教程。光盘具体使用方法请阅读下页的“光盘使用说明”。

本书由前沿文化与中国科技出版传媒集团新世纪书局联合策划。参与本书编创的人员都具有丰富的实战经验和一线教学经验，在此，向所有参与本书编创的人员表示感谢！

最后，真诚感谢读者购买本书。您的支持是我们最大的动力，我们将不断努力，为您奉献更多、更优秀的计算机图书！由于计算机技术发展非常迅速，加上编者水平有限，疏漏之处在所难免，敬请广大读者和同行批评指正。

编者

2012年5月



光盘使用说明

多媒体光盘内容

本书配套的多媒体教学光盘内容包括40个教学视频，视频教程对应书中各章节的内容，为各章节内容的操作步骤配音视频演示录像，播放时间长达150分钟。另外，随书附赠畅销书《电脑上网》、《电脑组装、维护与故障排除》和《系统安装、重装、备份与还原》的视频教程。读者可以先阅读图书再浏览光盘，也可以直接通过光盘学习电脑安全保障方法。

光盘使用方法

将本书的配套光盘放入光驱后会自动运行多媒体程序，并进入光盘的主界面，如图1所示。如果光盘没有自动运行，只需在“我的电脑”中双击光驱的盘符进入配套光盘，然后双击start.exe文件即可。

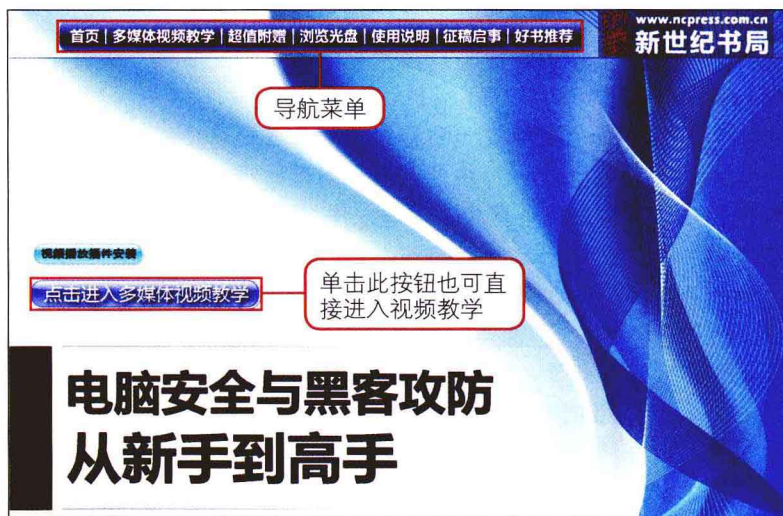


图1 光盘主界面

光盘主界面上方的导航菜单中包括“多媒体视频教学”、“浏览光盘”和“使用说明”等项目，如图1所示。单击“多媒体视频教学”按钮，可显示“目录浏览区”和“视频播放区”，如图2所示。“目录浏览区”用来显示书中所有视频教程的目录，“视频播放区”是播放视频文件的窗口。在“目录浏览区”中有以章序号顺序排列的按钮，单击按钮，将在下方显示以节标题命名的该章所有视频文件的链接。单击链接，对应的视频文件将在“视频播放区”中播放。

How to Use the CD-ROM



图2 显示视频信息

单击“视频播放区”中控制条上的按钮可以控制视频的播放，如暂停、快进；双击播放画面可以全屏幕播放视频，如图3所示；再次双击全屏幕播放的视频可以回到如图2所示的播放模式。

通过单击导航菜单（见图1）中不同的项目按钮，可以浏览光盘中的其他内容。

单击“使用说明”按钮，可以查看使用光盘的设备要求及使用方法。

单击“征稿启事”按钮，有合作意向的作者可与我社取得联系。

单击“好书推荐”按钮，可以看到本社近期出版的畅销书目录，如图4所示。



图3 全屏显示



图4 好书推荐



阅读帮助

知识加油站

提高性的知识和技巧，帮助您解决更多的问题



电脑安全与黑客攻防从新手到高手

之后关闭“注册表编辑器”进行测试，只需按照上述方法，再次打开“运行”对话框并启动“注册表编辑器”，即可弹出一个警告对话框，如下图所示。



如果没有对应值项怎么办

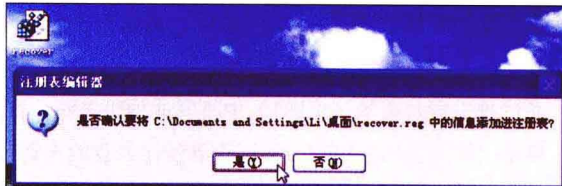
如果在定位值项时发现有些项或值可能不存在，此时用户可自行新建，效果是一样的。

那么，当用户要重新启动“注册表编辑器”时，怎么办呢？可以按照以下方法来解除之前的锁定。

打开“记事本”窗口，把以下代码保存到文档里。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System]
"DisableRegistryTools"=dword:00000000
```

将文档保存为recover.reg后，弹出一个确认对话框，单击“是”按钮即可，如下图所示。



疑难解答

主要对用户经常会出现的疑问进行解释



问：为什么保存的文件双击后，仍然是用“记事本”打开呢？

答：利用“记事本”保存文档，默认是保存为TXT格式的。即使在保存时输入文件名recover.reg，也会被保存为recover.reg.txt。这样一来，本质上还是一个文本文件，因此双击时仍然会用“记事本”打开。解决的方法：在保存时，先将“保存类型”设置为“所有文件”，然后再输入文件名，这样保存下来的文件，其扩展名不再是.txt，而是用户指定的.reg。

5.1.2

设置注册表防止系统隐私信息被泄露

视频教程见光盘

在前章中曾经提到过，当Windows系统运行出错时，系统内部有一个DR.WATSON程序会自动地将系统调用的隐私信息保存下来，隐私信息将保存在user.dmp和drwtsn32.log文件中。攻击者可以通过破解这个程序而了解系统的隐私信息，因此需要阻止该程序将信息泄露出去。

How to Read the Book



修改注册表中相应值项的值可阻止此程序自动运行，从而使其不再自动保存敏感信息，具体的操作步骤如下。

1 定位值项

1 打开“注册表编辑器”，并依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug；2 右击Auto值项；3 单击“修改”命令，如下图所示。



2 修改值项的值

1 在弹出的“编辑字符串”对话框的“数值数据”文本框中输入“0”；2 单击“确定”按钮，如下图所示。



5.1.3 关闭默认共享保护系统安全

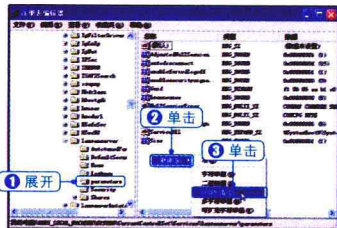
视频教程见光盘

Windows 2000/XP/2003版本的操作系统提供了默认共享功能，这些默认的共享都有“\$”标志，意为隐含的，包括所有的逻辑分区（C\$，D\$，E\$，...）和系统目录Winnt或Windows（admin\$）。如访问Windows XP的默认共享功能就非常简单：一是通过“运行”对话框输入“\\计算机名或IP地址\D\$或admin\$”（不包括两侧的引号）；二是使用IE等浏览器，在地址栏中输入上述格式或“file:\\IP地址\D\$”。

默认共享带来的问题：初衷本是便于网管进行远程管理，它虽然方便了局域网用户，但对个人用户来说这样的设置是不安全的——网络上的任何人都可以访问自己的共享硬盘，黑客也可以通过对这些默认共享的访问来进行信息窃取或入侵。因此，这些默认共享有必要关掉，具体操作步骤如下。

1 新建值项

1 打开“注册表编辑器”，并依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters；2 在右侧窗口的空白处单击鼠标右键，在弹出的快捷菜单中单击“新建”命令；3 单击“DWORD值”命令，如右图所示。



操作步骤

按照①、②、③……的顺序逐步操作，关键操作均在图上标注

光盘图标

提示光盘收录了与该实例配套的视频文件

目录

CONTENTS

Chapter

01

网络安全初接触 001

1.1 网络安全 002

1.1.1 网络安全的目的及保护范围 002

1.1.2 现有的网络攻击/防御手段 003

1.1.3 网络安全的四大方面 004

1.1.4 通过管理保护网络安全 005

1.1.5 网络安全的实施目的 008

1.2 了解常见的不安全因素 010

1.2.1 由网络系统本身带来的不安全
因素 010

1.2.2 网络外部的不安全因素 012

1.2.3 网络不安全的原因 014

1.3 认识网络安全的现状和 发展趋势 016

1.3.1 网络安全的现状 016

1.3.2 网络安全的发展趋势 017

Chapter

02

了解随处可见的计算机 病毒 019

2.1 计算机病毒的前世今生 020

2.1.1 什么是计算机病毒 020

2.1.2 计算机病毒起源何方 020

2.1.3 计算机病毒的发展历程 021

2.1.4 计算机病毒有哪些类型 025

2.1.5 计算机病毒的命名规则 028

2.1.6 解析计算机病毒的结构 028

2.1.7 计算机病毒的特征 031

2.2 计算机病毒如何作恶 032

2.2.1 计算机中毒后的表现 032

2.2.2 如何防范计算机病毒 034

2.3 常见计算机病毒类型详解 036

2.3.1 引导型病毒 036

2.3.2 文件型病毒 037

2.3.3 宏病毒 038

2.3.4 蠕虫病毒 039



Chapter 03

揭开黑客与木马的面纱……041

3.1 什么是黑客……042

- 3.1.1 “尼奥”们的由来……042
- 3.1.2 黑客和骇客的区别……043
- 3.1.3 黑客活动历史……044
- 3.1.4 我国黑客发展历程……046

3.2 黑客攻击的类型与动机……047

- 3.2.1 攻击目的……047
- 3.2.2 攻击动机……049

3.3 木马的历史渊源……050

- 3.3.1 希腊美女海伦与木马……050
- 3.3.2 什么是计算机木马……050
- 3.3.3 木马工作类型……054
- 3.3.4 木马的发展历程……056
- 3.3.5 经典木马介绍……057

3.4 木马的追踪与防范……059

- 3.4.1 木马的追踪与反追踪技术……059
- 3.4.2 木马的防范方法……060

Chapter 04

掌握Windows系统的漏洞…062

4.1 Windows系统的安全隐患…063

- 4.1.1 Windows系统漏洞产生的原因……063
- 4.1.2 Windows系统中的安全隐患……064

4.2 Windows系统中的漏洞……067

- 4.2.1 UPnP服务漏洞……067
- 4.2.2 升级程序漏洞……068
- 4.2.3 帮助和支持中心漏洞……068
- 4.2.4 Windows Media Player漏洞……068
- 4.2.5 压缩文件夹漏洞……069
- 4.2.6 服务拒绝漏洞……069
- 4.2.7 RDP漏洞……069
- 4.2.8 VM漏洞……070
- 4.2.9 热键漏洞……070

- 4.2.10 账号快速切换漏洞……070
- 4.2.11 输入法漏洞……071
- 4.2.12 Unicode漏洞……071
- 4.2.13 ISAPI缓冲区扩展溢出漏洞……072
- 4.2.14 MS SQL Server的SA空密码漏洞……072
- 4.2.15 系统管理权限漏洞……073
- 4.2.16 路径优先漏洞……073
- 4.2.17 NetDDE消息权限提升漏洞……074
- 4.2.18 RDP拒绝服务漏洞……074
- 4.2.19 域控制器拒绝服务漏洞……075
- 4.2.20 事件查看器存在缓冲区溢出漏洞……075
- 4.2.21 UDP套接字拒绝服务漏洞……075
- 4.2.22 安全账户管理漏洞……075

4.2.23 IIS 5.0的HTR映射远程堆溢出漏洞	076	4.2.43 IIS 5.0 Cross Site Scripting漏洞	083
4.2.24 IIS 5.0的ASP缓冲溢出漏洞	076	4.2.44 组策略漏洞	083
4.2.25 Narrator本地密码信息泄露漏洞	077	4.2.45 数字签名缓冲区溢出漏洞	083
4.2.26 SMTP认证漏洞	077	4.3 针对漏洞的入侵方式	084
4.2.27 IIS 5.0/5.1验证漏洞	077	4.3.1 数据驱动攻击	084
4.2.28 SQL Server函数数据库漏洞	077	4.3.2 伪造信息攻击	084
4.2.29 IIS 5.0伪造拒绝服务漏洞	078	4.3.3 针对信息协议弱点攻击	084
4.2.30 调试寄存器漏洞	078	4.3.4 登录欺骗	084
4.2.31 drwtsn32.exe文件漏洞	078	4.3.5 利用系统管理员失误攻击	084
4.2.32 快捷方式漏洞	079	4.3.6 重新发送攻击	085
4.2.33 UTF漏洞	079	4.3.7 ICMP报文攻击	085
4.2.34 IIS 5.0的SEARCH方法存在远程攻击漏洞	079	4.3.8 针对源路径选项的弱点攻击	085
4.2.35 Telnet漏洞	080	4.3.9 以太网广播攻击	085
4.2.36 LDAP漏洞	080	4.4 掌握常用的防护方法	085
4.2.37 IIS 5.0拒绝服务漏洞	081	4.4.1 杀毒软件不可少	086
4.2.38 默认注册许可漏洞	081	4.4.2 个人防火墙不可替代	086
4.2.39 登录服务恢复模式存在空密码漏洞	081	4.4.3 分类设置复杂密码	086
4.2.40 域账号锁定漏洞	082	4.4.4 防止网络病毒与木马	086
4.2.41 终端服务器登录缓存溢出漏洞	082	4.4.5 警惕“网络钓鱼”	087
4.2.42 ActiveX参数漏洞	082	4.4.6 防范间谍软件	087
		4.4.7 只在必要时共享文件夹	087
		4.4.8 定期备份重要数据	087

Chapter 05

Windows系统漏洞的防范 妙招 088

5.1 注册表安全防范技巧	089	 5.1.1 禁止访问和编辑注册表	089
----------------------------	------------	---	------------



 5.1.2 设置注册表防止系统隐私信息 被泄露.....090	 5.2.3 密码策略.....100
 5.1.3 关闭默认共享保护系统安全.....091	5.2.4 禁止更改桌面设置.....103
5.1.4 设置登录警告.....092	5.2.5 隐藏“我的电脑”中指定的 驱动器.....103
5.1.5 隐藏桌面所有图标.....092	5.2.6 防止从“我的电脑”访问 驱动器.....103
5.1.6 清理自动启动的程序.....093	5.2.7 禁止使用命令提示符.....104
5.1.7 禁用“刻录”功能.....094	5.2.8 禁止更改显示属性.....104
5.1.8 删除“开始”菜单中的 “文档”项.....094	5.2.9 禁用注册表编辑器.....104
5.1.9 删除查找结果中的文件列表.....094	5.2.10 彻底禁止访问“控制面板”.....105
5.1.10 在“我的电脑”中屏蔽磁盘 驱动器图标.....094	5.2.11 禁止建立新的拨号连接.....105
5.1.11 清理访问“网上邻居”后 留下的信息.....095	5.2.12 禁用“添加/删除程序”.....105
5.1.12 删除“运行”窗口中多余的 选项.....095	 5.2.13 限制使用应用程序.....105
5.1.13 在桌面上隐藏“网上邻居” 图标.....095	5.3 设置系统中的各类密码.....107
5.1.14 禁止运行任何程序.....096	 5.3.1 设置Windows登录密码.....107
5.1.15 禁止远程修改注册表.....096	 5.3.2 设置电源管理密码.....108
5.2 组策略安全登录设置.....097	 5.3.3 设置屏幕保护程序密码.....109
 5.2.1 设置休眠/挂起密码.....097	5.4 掌握Windows XP的安全 设置方法.....111
 5.2.2 账户锁定策略.....098	 5.4.1 充分利用防火墙功能.....111
	5.4.2 启用自动更新.....112
	 5.4.3 禁止病毒启动系统服务.....112
	 5.4.4 快速锁定计算机.....113

Chapter

06

黑客常用命令详解.....115

6.1 认识IP地址.....116	6.1.4 公有IP地址与私有IP地址.....118
6.1.1 什么是IP地址.....116	6.2 计算机通向外界的道路—— 端口.....119
6.1.2 IP地址的划分.....116	6.2.1 端口的分类.....119
6.1.3 分配IP地址的机构.....118	



6.2.2 查看端口121

6.2.3 端口的关闭与限制121

6.3 黑客常用命令一览.....124

6.3.1 net命令125

6.3.2 远程登录命令telnet127

6.3.3 文件传输命令ftp128

6.3.4 添加计划任务命令at129

6.3.5 查看修改文件夹权限
命令cacls130

6.3.6 回显命令echo131

6.3.7 命令行下的注册表操作131

6.3.8 查看当前系统用户情况
命令query132

6.3.9 终止会话命令logoff.....132

6.3.10 物理网络查看命令ping.....133

6.3.11 网络配置查看命令ipconfig.....134

6.3.12 DNS查看命令nslookup.....135

6.3.13 地址解析命令arp135

Chapter

07

搜集远程计算机的信息 137

7.1 搜集网络中的信息.....138

7.1.1 获取目标计算机的IP地址138

7.1.2 由IP地址获取目标计算机的
地理位置139

7.1.3 了解网站备案信息139

7.2 检测系统漏洞.....141

7.2.1 什么是扫描器.....141

7.2.2 搜索共享资源.....142

7.3 端口扫描143

7.3.1 端口扫描的原理与分类143

7.3.2 端口扫描工具X-Scan146

Chapter

08

远程入侵计算机 148

8.1 基于认证的入侵149

8.1.1 IPC\$入侵149

8.1.2 Telnet入侵155

8.1.3 防范IPC\$连接入侵.....161

8.2 利用注册表入侵165

8.2.1 开启远程注册表服务.....165

8.2.2 连接远程注册表167

8.2.3 通过注册表开启终端服务168

8.3 常见问题解答.....168



Chapter

09

木马入侵与防御 170

9.1 深入了解木马 171

9.1.1 木马常用的入侵手法 171

 9.1.2 深入了解木马的伪装手段 172

9.1.3 识别木马有招数 174

9.1.4 防范木马的入侵 175

9.2 木马的捆绑与使用 176

 9.2.1 使用Exebinder捆绑木马 176 9.2.2 经典木马“冰河”的使用方法 179

Chapter

10

QQ攻击与防御 183

10.1 远程攻击QQ 184

 10.1.1 强制聊天 18410.1.2 使用“QQ狙击手IpSniper”
进行IP探测 185 10.1.3 使用QQ炸弹攻击器进行
信息轰炸 186

10.2 本地入侵QQ 187

 10.2.1 使用QQ聊天记录器记录
聊天内容 187

10.2.2 强行查看本地QQ聊天记录 188

10.2.3 破解本地QQ密码 189

10.3 QQ防御术 190

10.3.1 防止QQ密码被破解 190

 10.3.2 防范IP地址被探测 192

10.3.3 防范QQ炸弹和木马 193

Chapter

11

电子邮箱攻击与防御 195

11.1 获取电子邮箱密码的常用
方法 19611.1.1 使用“流光”软件探测邮箱
账号与密码 19611.1.2 使用“溯雪”软件获取邮箱
密码 20011.1.3 使用“Email网页神抓”软件
大批量获取邮箱地址 203 11.1.4 对付密码探测的方法 20411.2 电子邮箱攻击手段与
防范 207

11.2.1 使用邮箱炸弹进行攻击 207

 11.2.2 对付邮箱攻击的方法 207



Chapter
12

来自网页的攻击与防御方法 211

12.1 了解恶意代码 212	12.2.8 Outlook标题栏被添加广告信息 218
12.1.1 恶意代码的特征 212	12.2.9 IE右键菜单被添加非法网站链接 218
12.1.2 非过滤性病毒 212	12.2.10 单击鼠标右键弹出菜单功能被禁用 218
12.1.3 恶意代码的传播方式 213	12.2.11 地址栏的下拉菜单被锁定并被添加文字信息 219
12.1.4 恶意代码的传播趋势 214	12.2.12 IE“查看”菜单下的“源文件”项被禁用 219
12.2 解除恶意代码对注册表的攻击 215	12.2.13 系统启动时弹出对话框 219
12.2.1 开机后自动弹出网页 215	12.3 危险的IE浏览器 219
12.2.2 浏览网页注册表被禁用 215	12.3.1 IE炸弹攻击类型与后果 220
12.2.3 IE标题栏、默认首页被强行修改 216	 12.3.2 对IE炸弹的防范与补救 220
12.2.4 默认的微软主页被修改 216	12.4 网页攻击与防范实例 222
12.2.5 主页设置被屏蔽锁定且设置选项无效不可更改 216	12.4.1 常见ASP脚本攻击与防范 222
12.2.6 默认的IE搜索引擎被修改 217	12.4.2 跨站攻击和防范 222
12.2.7 IE标题栏被添加广告信息 217	

Chapter
13

防范扫描与恶意软件 225

13.1 保护IP和端口 226	13.2 清除恶意广告软件 233
 13.1.1 设置代理服务器 226	13.2.1 使用Ad-Aware驱逐恶意广告软件 234
 13.1.2 关闭端口 227	 13.2.2 使用安博士软件驱逐恶意广告 235
 13.1.3 配置安全策略保护端口 228	

**13.3 清除木马235**

- 13.3.1 使用Windows任务管理器
管理进程236
- 13.3.2 使用Trojan Remover清除
木马238

- 13.3.3 使用Unlocker删除顽固
木马文件239
- 13.3.4 使用360安全卫士维护
系统安全240

Chapter**14****网站攻防入门242****14.1 网站安全详解243**

- 14.1.1 网络攻击与网站243
- 14.1.2 网站安全与“肉鸡”243
- 14.1.3 动态网站与网站安全244
- 14.1.4 数据库与网站安全245
- 14.1.5 SQL与网站安全248
- 14.1.6 Web 2.0网站与黑客249
- 14.1.7 网站服务249
- 14.1.8 客户端交互技术Ajax250

14.2 网站的结构和组成251

- 14.2.1 网站系统基本架构251
- 14.2.2 网站工作原理252
- 14.2.3 网站服务器252
- 14.2.4 网页浏览器252

14.3 网页程序开发语言分类252

- 14.3.1 服务器端开发语言252
- 14.3.2 客户端开发语言253

**14.4 网站程序运行的常见
环境254**

- 14.4.1 Windows下的网站运行
平台255
- 14.4.2 Linux下的网站运行平台255

**14.5 网站程序常见错误提示的
含义257**

- 14.5.1 HTTP错误提示含义258
- 14.5.2 FTP错误提示含义260

14.6 网站程序数据通信方式262

- 14.6.1 URL与HTTP/HTTPS协议262
- 14.6.2 Cookies与Session264
- 14.6.3 GET与POST数据提交264
- 14.6.4 常用字符集分类265

14.7 网站程序数据加密方式266

- 14.7.1 MD5加密267
- 14.7.2 SHA1加密268
- 14.7.3 Base64加密268
- 14.7.4 Zend加密269
- 14.7.5 ASP代码加密工具269

14.8 常见网站漏洞一览270



Chapter

15

网站上传漏洞的攻击和防御 271

15.1 上传漏洞存在的原因 272

15.2 各种类型的上传漏洞 273

15.2.1 上传路径过滤不严导致的漏洞 274

15.2.2 上传文件类型变量过滤不严造成的漏洞 276

15.2.3 文件名过滤不严造成的漏洞 278

15.2.4 逻辑错误产生的漏洞 279

15.3 各种在线编辑器漏洞 281

15.3.1 突破图片预览的限制 282

15.3.2 突破禁止创建.asp文件夹的限制 282

15.3.3 增加上传图片类型 283

15.3.4 反过滤上传 284

15.4 上传漏洞的防御 284

15.4.1 下载官方补丁 284

15.4.2 找网站开发商修改程序来防御上传漏洞 286

15.4.3 换用其他编辑器的方法来防御上传漏洞 286

15.4.4 用手动法来防御上传漏洞 286

Chapter

16

网站脚本注入的攻击与防御 288

16.1 深入剖析脚本注入攻击 289

16.1.1 注入攻击核心原理 289

16.1.2 形式各异的注入攻击分类 289

16.1.3 SQL注入攻击特点 289

16.1.4 注入攻击流程详解 290

16.2 注入攻击的基础 292

16.2.1 数据库知识 292

16.2.2 SQL注入与数据库 294

16.3 注入漏洞案例剖析 300

16.3.1 ASP注入漏洞案例分析 300

16.3.2 ASPX注入漏洞案例分析 301

16.3.3 PHP注入漏洞案例分析 303

16.4 防御注入攻击 306

16.4.1 提高编程水平 306

16.4.2 提高密码的复杂程度 307

16.4.3 善用防注入工具 307