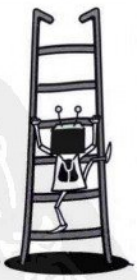
www.ncpress.com.cn
新世纪书局

1CD 多媒体教学光盘
40段视频教程，时间长达150分钟
附赠《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从新手到高手

前沿文化/编著



内容全面实用 讲解清晰易懂

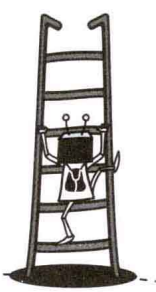
彩色图书 视频光盘 超值附赠

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从新手到高手

前沿文化/编著



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）

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。

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

疑难解答

主要对用户经常会出现的疑问进行解释

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”，即可会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。

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

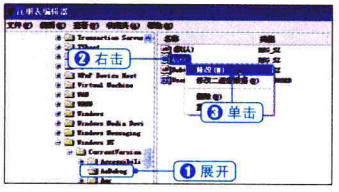
在前章中曾经提到过，当Windows系统运行出错时，系统内部有一个DR.WATSON程序会自动地将系统调用的隐私信息保存下来，隐私信息将保存在user.dmp和drwtsn32.log文件中。攻击者可以通过破解这个程序而了解系统的隐私信息，因此需要阻止该程序将信息泄露出去。

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

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



2 修改值项的值

❶ 在弹出的“编辑字符串”对话框的“数值数据”文本框中输入“0”；❷ 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

❶ 打开“注册表编辑器”，并依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters；❷ 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；❸ 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