EASY TO LEARN

懂与不懂的距离，只有24小时……

24 Hours 小时学会

全彩印刷

黑客攻防

◎ 导向工作室 编著

- **科学设计，自主安排**
  24小时课程规划，全面覆盖黑客攻防知识技能。
- **实例精讲，极速上手**
  密切结合黑客攻击与防御，讲练结合，学完就用。
- **视频讲解，名师相伴**
  多媒体立体化教学，木马密码攻防、软件漏洞攻防、系统安全防御，得心应手。
- **独家技巧，精妙总结**
  十大安全性防护守则、十大网络技巧、十大防御黑客攻击方法，倍。

对应24小时课程
立体化视频教学
多媒体光盘巨献

人民邮电出版社
POSTS & TELECOM PRESS

EASY TO LEARN

24小时

Hours

学会黑客攻防

◎ 导向工作室　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

24小时学会黑客攻防 / 导向工作室编著. -- 北京 : 人民邮电出版社, 2011.5
ISBN 978-7-115-24696-7

Ⅰ. ①2… Ⅱ. ①导… Ⅲ. ①计算机网络－安全技术
Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2011)第027482号

内 容 提 要

本书以如何防御黑客的攻击为线索，详细而又全面地介绍了黑客攻击电脑和防御黑客攻击的相关知识。主要内容包括：黑客攻防基础、木马程序的攻击与防御、电脑中各种密码的破解与防御、各种常见软件的攻击与防御、系统漏洞的攻击与防御和电脑系统的安全防御等，本书的最后一篇还总结了防御黑客攻击的常见问题及解决方法，供读者参考。

本书附带的多媒体光盘中，赠送了与24小时学习计划相对应的视频教学软件，帮助读者在立体化的学习环境中，取得事半功倍的学习效果。

本书适合电脑维护人员、IT从业人员及对黑客攻防和安全维护知识感兴趣的电脑初、中级用户阅读，也可作为各种电脑培训班的教材或辅导用书。

24小时学会黑客攻防

◆ 编　　著　导向工作室
责任编辑　张　翼
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫丰华彩印有限公司印刷
◆ 开本：880×1230　1/32
印张：7
字数：340 千字　　2011年5月第1版
印数：1－8 000 册　　2011年5月北京第1次印刷

ISBN 978-7-115-24696-7

定价：24.80 元（附光盘）

读者服务热线：(010)67132705　印装质量热线：(010)67129223
反盗版热线：(010)67171154
广告经营许可证：京崇工商广字第0021号

前言

本书能让你学会什么？

- 密码的攻击和防御
- 木马程序的攻击和防御
- 电子邮件的攻击和防御
- 常用软件的攻击和防御
- 电脑的安全防御

黑客，对于普通电脑用户来说，太神秘，也太可恨了，他们通过各种方法侵入我们的电脑，窃取电脑中的信息。很多时候，普通电脑用户在对黑客痛恨的同时，又钦佩其高超的电脑技术，从而想了解黑客是如何攻击电脑的，并掌握防御黑客攻击的方法，为电脑系统和网络的安全贡献自己的一份力量。

本书从实用的角度出发，全面、详细地讲解了黑客攻击和如何防御黑客攻击的相关内容。通过对本书的学习，广大电脑用户能够在短时间内轻松掌握保护电脑安全的方法和技巧。

内容导读

全书分为7篇，共计24小时的学习计划，各篇主要内容介绍如下。

第1篇 黑客攻防基础：介绍了黑客攻防的准备知识，包括了解黑客、黑客攻防的准备工作、黑客常用的攻击工具和黑客对网站信息的收集等。

第2篇 木马攻防：介绍了黑客利用木马攻击和如何防御木马攻击的知识，包括木马的基础知识、木马如何攻击和防御木马入侵等。

第3篇 密码攻防：介绍了黑客破解各种密码和保护密码的知识，包括黑客如何破解各种密码、保护电脑中的密码和QQ密码的破解与保护等。

第4篇 常用软件攻防：介绍了常用软件的攻击和防御的相关知识，包括QQ软件的攻击、电子邮件的攻击与防御和IE浏览器的攻击与防御等。

第5篇 系统漏洞攻防：介绍了攻击系统漏洞和防御攻击的方法，包括认识一些常见的系统漏洞、攻击系统漏洞和系统漏洞防御等。

第6篇 安全防御：介绍了普通电脑用户如何进行安全防御的操作与方法，包括防御恶意入侵、如何设置操作系统、设置注册表、备份与还原系统盘、备份与恢复电脑中的数据和使用安全防御软件等。

第7篇 “十大”技巧精选：介绍了防御电脑系统安全的方法，包括来自Microsoft的十大安全性防御守则、网络管理员必备的十大安全技巧和ADSL防御黑客攻击的十大方法等。

本书特点

科学的学习计划：本书共计24小时学习内容，帮助读者建立科学的学习计划；读者既可以跟随本书按部就班地学习，也可以根据个人情况自主安排学习进度。

务实的案例设计：本书紧扣实际应用，通过案例进行讲解，同时提供了丰富的拓展练习，满足读者的实际需求。

全面的知识覆盖：本书除知识主线以外，还穿插了大量的“小提示”、“长见

识”等栏目，随时提供操作技巧及扩展知识，帮助读者巩固提高。

配套的视频讲解：本书配套的多媒体光盘中，赠送了与24小时学习计划对应的同步视频软件，立体化教学，全方位指导。

实用的技巧总结：本书最后一篇中，结合作者经验及广大用户的使用心得，精心总结了若干技巧和注意事项等，帮助读者事半功倍地掌握电脑技能。

精美的排版印刷：本书使用全彩印刷，双栏排版，图文对应，整齐美观，便于读者查看和学习。

读者对象

本书适合电脑维护人员、IT从业人员及对黑客攻防和安全维护知识感兴趣的电脑初、中级用户阅读，也可作为各种电脑培训班的教材或辅导用书。

关于我们

本书由导向工作室组织编写，参与本书资料收集整理、编写、校对及排版的人员有：蔡飓、肖庆、李秋菊、黄晓宇、蔡长兵、刘波、牟春花、王维、赵莉、熊春、李洁羽、蒲乐、马鑫、耿跃鹰、李枚锏、于昕杰、高志清、卢妍等。如果您有什么关于本书的疑问或改进建议，可通过E-mail（dxts@foxmail.com）与我们联系。

由于作者水平有限，书中疏漏和不足之处在所难免，欢迎广大读者朋友批评指正。

导向工作室

2011年3月

多媒体光盘使用说明

多媒体光盘内容

本书配套多媒体光盘中包含144个重点操作的视频教程以及17个“跟我上机”练习的参考操作动画演示，与书中“24小时”学习计划相对应。学习过程包括“演示”和“操作”两种模式。在“演示”模式中，读者可以观看具体的操作演示过程；在“操作”模式中，读者可以根据系统的提示，亲自动手进行演练。

光盘使用方法

将本书的配套多媒体光盘放入光驱后，光盘会自动运行并进入其主界面，如图1所示。如果光盘没有自动运行，只需在“我的电脑”窗口中双击光驱的盘符打开光盘，在光盘的根目录中双击“autorun.exe”文件即可。

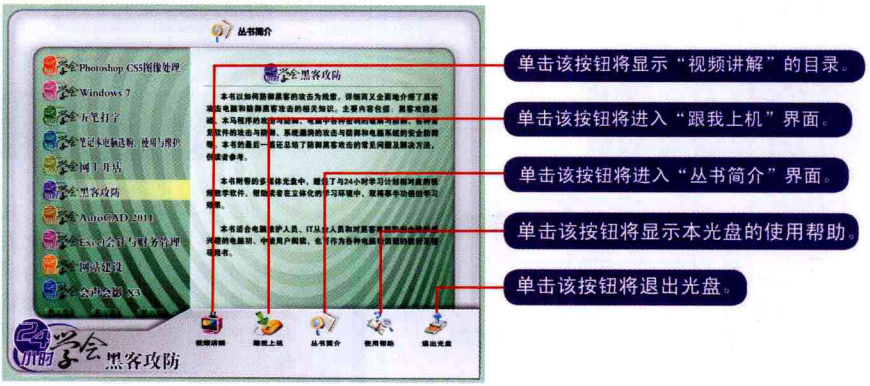


图 1

单击“视频讲解”按钮，将显示视频讲解的目录，如图2所示。用鼠标单击要观看的章节的标题即可进入视频播放界面，开始学习相应的内容。

图 2

视频播放界面如图3所示，系统在播放完一个视频文件后，会自动播放下一个视频文件。

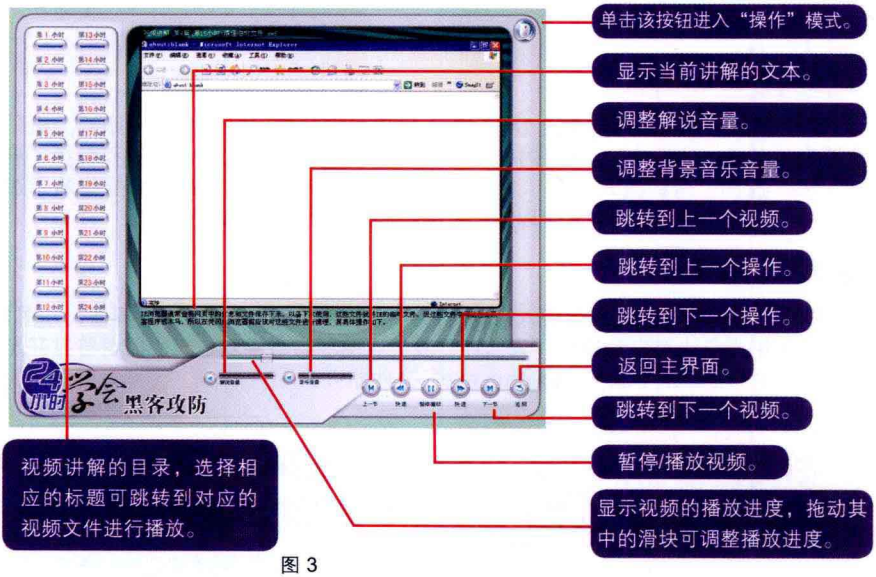
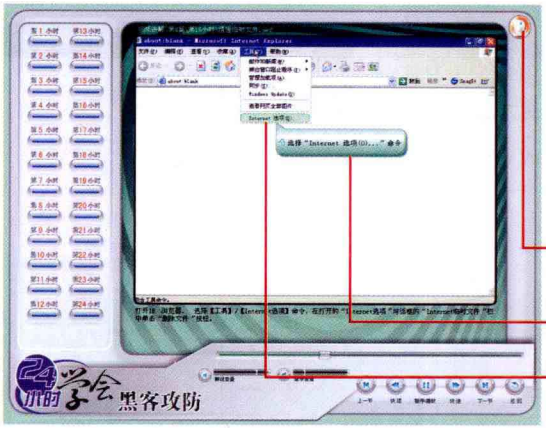


图 3



单击“操作模式”按钮，将进入操作模式，此时“操作模式”按钮将变为黄色，如图4所示，读者可根据系统的操作提示进行实际操作。

图4

本光盘最佳运行环境

- CPU：Pentium 4 及以上。
- 内存：512 MB及以上。
- 硬盘剩余空间：200 MB及以上。
- 屏幕分辨率：1024 像素 × 768像素。
- 其他：52倍速以上光驱，或4倍速以上DVD光驱。

目录

第 1 篇 黑客攻防基础

第 2 篇 木马攻防

第3篇 密码攻防

第 4 篇 常用软件攻防

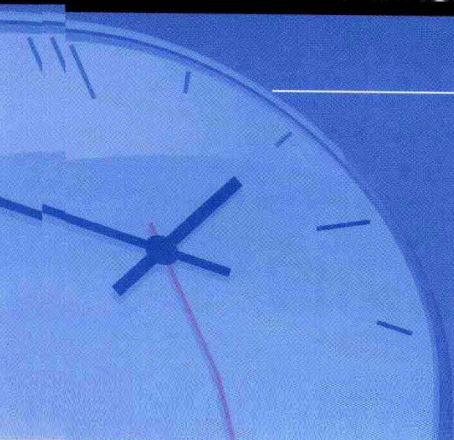
第5篇 系统漏洞攻防

第6篇 安全防御

第1篇

黑客攻防基础

无论是想要充分了解黑客，还是要防御黑客的进攻，都需要首先了解一些与黑客相关的基础知识，比如黑客的定义、发展历史和攻击目的，以及黑客通常了解的一些基本知识等。所以，本篇将主要讲解黑客的基本情况、黑客攻防的准备工作、黑客常用的攻击工具和命令，以及收集各种信息等知识，帮助大家为学习黑客攻防打下坚实的基础。



4小时学习目标

- 了解黑客
- 黑客攻防的准备工作
- 黑客常用的攻击工具
- 黑客对网站信息的收集

第1小时 了解黑客

学习黑客攻防，首先应该了解黑客的相关知识，如认识黑客的发展历史，黑客攻击的基本流程，黑客常用的理论知识等。

参见随书光盘 视频讲解\第1篇\第1小时

什么是黑客

对于大多数人来说，黑客是神秘和无所不能的代表，其实不然。下面就帮助大家了解黑客，以及黑客的发展历史、现状与未来、行为准则和精神素质等知识。（视频讲解参见：什么是黑客.swf。）

1. 黑客的定义

黑客是英文单词“hacker”的中文翻译，本意是指热衷于计算机技术、水平高超的电脑专家和程序设计人员。而现在，因对待系统、网络和软件中安全漏洞态度的不同将其分为两类：一类黑客会找出并弥补这些漏洞；但另一类黑客则在找出安全漏洞之后，为了显示自己的本领和成就，对别人的电脑大肆进行恶意破坏。总的来说，对于“黑客”一词，一般有以下几种意义。

意义一

对（某领域内的）编程语言有足够了解，可以编写出有价值的程序的人。

意义二

恶意（通常是非法地）试图破解或破坏某个程序、系统及安全密码的人。这个意义常常对那些符合第一种意义的黑客造成严重困扰，通常媒体将这群人称为“骇客”（cracker），有时这群人也被叫做“黑帽黑客”。

意义三

通过知识或直觉而对某段程序做出（好的）修改，并完善（或增强）该程序用途的人。

意义四

试图通过漏洞破解系统或网络，以提醒创造者或修系统的人，这种往往被称作“白帽黑客”或“匿名客”（sneaker）或“红客”。这样的人大多是电脑安全公司的雇员，他们在完全合法的情况下攻击系统漏洞或网络。

2. 黑客的发展历史

黑客的起源可以追溯到20世纪50年代，主要分为以下几个阶段。

20世纪50年代

通常认为黑客起源于20世纪50年代麻省理工学院的实验室中，这些黑客主要目的是解决各种电脑难题。

20世纪60年代

60年代后，黑客是指善于独立思考且奉公守法的电脑爱好者，他们利用分时技术允许多个用户同时执行多道程序，扩大了电脑及网络的使用范围。

20世纪70年代

70年代后，在黑客们的技术支持下，发明并生产了个人电脑，打破了以往电脑技术只掌握在少数人手里的局面，并提出了电脑为大众所用的观点。通常也把这一时代的黑客看成是电脑史上的英雄，同时，一些黑客也发明了一些侵入电脑系统的基本口令和技巧，如破解口令、开天窗、进入后门和安装木马程序等。

20世纪80年代

80年代的软件工程师就是黑客的代表，这一代黑客为个人电脑编写出了各种应用软件。而就在此时，随着各种大型数据库的建立（但这些信息不能被公开使用），黑客开始分化，一部分黑客通过自己的技术为信息共享而奋斗，另一部分黑客则开始频繁的入侵各大电脑网络。

20世纪90年代至今

现在的黑客种类很多，具有代表性的有如下几类：善意的以发现计算机系统漏洞为乐趣的“电脑黑客”（Hacke）；玩世不恭好恶作剧的“电脑黑客”（Cyberbunk）；纯粹以私利为目的，任意篡改数据，非法获取信息的“电脑黑客”（Cracker）。

小提示：中国黑客发展史

在中国Internet技术的成长道路上，中国黑客与安全事业的发展历程也是交织在一起的，国内黑客的发展主要可分为中国黑客的起源（1994年-1996年）、中国黑客的成长（1997年-1999年）和中国黑客的发展（2000年至今）3个阶段。

3. 黑客的现状

我国的黑客起步较晚，但速度很快，目前的状况可以概括为以下四个方面。

良莠不齐

国内的黑客组织较多，但良莠不齐，很多人以一些简单程序迷惑不知情的网民，甚至打着黑客的旗号招摇撞骗，而真正为网络技术服务的很少。

普遍具有违法犯罪行为

大部分黑客都通过病毒和木马对网络中的电脑进行攻击，通过偷盗账号或密码破坏网络中的电脑，甚至进行各种经济犯罪，严重地制约了电子商务和网络支付等交易类市场的发展。

缺乏社会责任感

不少黑客攻击网络的目的在于炫耀个人的技术实力，没有意识到自己身上肩负的社会责任与时代使命，缺乏危机意识，甚至为违法犯罪分子所利用。

积极作用较少

从另一方面说，黑客攻击对网络安全起到了技术促进的作用，没有黑客，就没有现在的网络安全技术。同时，一批黑客高手已转变为网络安全专家，研发出众多安全技术和安全软件，对我国电脑或网络的发展做出了贡献。

4. 黑客的未来

针对我国黑客的现状，未来的发展应该注意以下几点。

明确目标

黑客应首先明确其自身的目标，以及黑客存在的价值观念，把维护国家和人民利益作为最高准则，建立起维护国家网络安全的阵线，大量培养信息后备人才，并激发人民的参与热情。

建立并完善制度

对于黑客组织来说，应结合活动规则，建立一套现代条件下的“黑客制度”。

与犯罪行为明确划清界限

黑客组织需要严厉打击犯罪行为。

长见识： 中国黑客联盟自1999年创建至今，已经历了十几个年头，为中国网络事业留下了不可磨灭的印象，也因此成就了众多的网络安全专家。

5. 黑客守则

黑客应该为社会安定贡献自己的力量，并遵守以下几点守则。

守则一
不入侵或破坏政府机关的主机。

守则二
不破坏他人的文件或数据。

守则三
不轻易将自己攻击的站点告诉其他人。

守则四
不要使用真名。

守则五
不在电话中谈论关于黑客的任何事情。

守则六
除非经过允许，不入侵或攻击各种正常网站的主机。

守则七
不修改他人电脑中的系统文件，如果目的是为了要进入系统而修改它，请在达到目的后将其还原。

守则八
不恶意破坏任何的系统。

守则九
不将已破解的账户公开。

守则十
不在网络上谈论关于黑客的任何事情。

守则十一
入侵期间，不随意离开电脑。

守则十二
不得删除或修改已入侵电脑的账号。

守则十三
阅读所有有关系统安全或系统漏洞的文件。

守则十四
不修改系统文件，如果为了隐藏自己的侵入而作的修改则不在此限，但仍需维持原来系统的安全性，不得因得到系统的控制权而破坏原有的安全性。

6. 黑客精神和素质

遵守了黑客守则的并不一定都是黑客，真正的黑客应该具备以下一些精神和素质。

素质一
不断地解决各种电脑问题。

素质二
不断地发现新的电脑问题。

素质三
追求创新。

素质四
编写免费的软件。

素质五
帮忙测试和完善免费的软件。

素质六
公布有用的电脑信息。

素质七
虚心接受他人的建议和意见。

素质八
具有良好的心理素质。

素质九
帮助维持网络和电脑的一些简单工作。

素质十
有明确的人生目标，并为之努力奋斗。

黑客的攻击流程

一般来说，普通黑客在对电脑进行攻击的流程是大致相同的，主要包括以下几个步骤。