KH 北京科海
25年 · IT技术出版专家

黑客
教学基地

-最新- COMPUTER HACKER

黑客攻防实战

从入门到精通

洞悉黑客机密 · 精通黑客攻防

武新华 翟长霖 安向东 编著

- 以黑客入侵过程为主线，深入剖析黑客攻防的各种最新手法。
- 任务驱动式教学，让你在边学边练中快速提高实战技能。
- 采用最为通俗易懂的图文解说，即使你是计算机新手也能通读全书。

情境式多媒体语音教学光盘

- 全程语音讲解+视频操作演示。
- **29**课全程情境式实战教学录像，让你轻松学会各种攻防技术。

科学出版社
北京科海电子出版社
www.khp.com.cn

-最新-

黑客攻防实战

从入门到精通

洞悉黑客机密 · 精通黑客攻防

武新华 翟长霖 安向东 编著

科学出版社
北京科海电子出版社
www.khp.com.cn

内 容 提 要

本书以黑客入侵过程为主线，循序渐进地介绍了黑客攻击计算机的一般方法、步骤、所使用的工具，以及防止黑客攻击的方法。主要内容包括：安全的虚拟机测试环境、踩点侦察与漏洞扫描、系统账户与口令密码、远程控制攻防技术、常见漏洞入侵工具使用、网络欺骗与突破限制、常见木马攻防实战、网络系统漏洞入侵渗透与防御、系统进程与隐藏技术和流氓软件与间谍软件的防范与清除，使读者提高网络安全意识，在遭遇黑客入侵时能够尽量做到心中有数，采取相关的自救措施。

本书由一线系统与网络安全技术专业人士编写，并提供多媒体语音视频教程。适用于黑客技术初学者、广大计算机安全技术爱好者、网络安全从业人员及网络管理员使用。

图书在版编目（CIP）数据

最新黑客攻防实战从入门到精通 / 武新华，翟长霖，安向东编著. —北京：科学出版社，2009

ISBN 978-7-03-024145-0

Ⅰ. 最… Ⅱ. ①武… ②翟… ③安… 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026593号

责任编辑：张少波 / 责任校对：刘雪莲

责任印制：科 海 / 封面设计：林 陶

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

北京市艺辉印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2009年4月第一版 开本：16开

2009年4月第一次印刷 印张：21.5

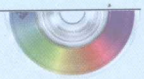
印数：0 001~4 000 字数：516 000

定价：36.00元（含1CD价格）

(如有印装质量问题，我社负责调换)

多媒体教学光盘使用说明

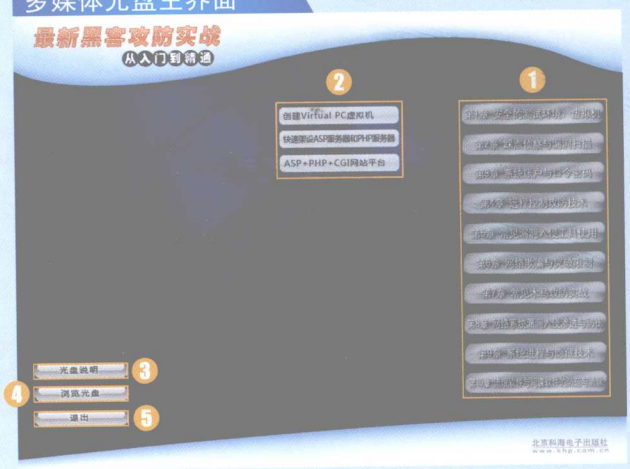
本书光盘包括



● 本书光盘包括29个书中实例的多媒体视频教程，全程语音讲解＋视频动画演示，总教学时间近3小时。

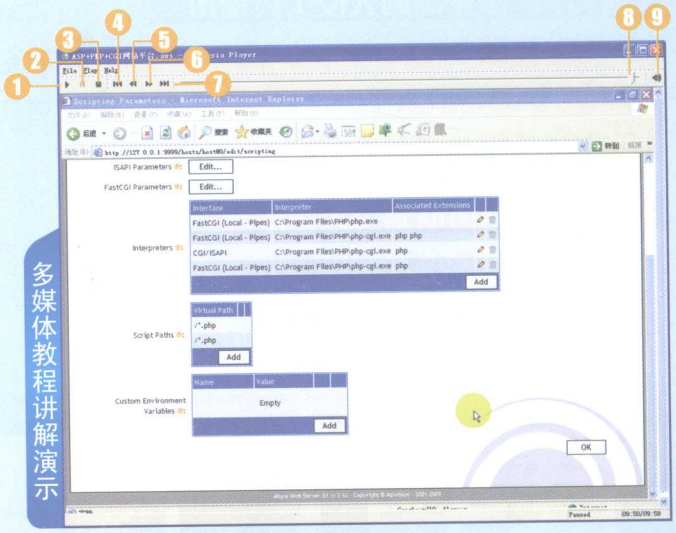
1. 多媒体教程主菜单（单击可显示二级菜单）
2. 二级菜单（单击可打开相应播放文件）
3. 单击可查看光盘说明
4. 单击可浏览光盘内容
5. 单击可退出播放程序

多媒体光盘主界面



1. 单击可播放视频
2. 单击可暂停播放视频
3. 单击可停止播放视频
4. 单击可返回起始点
5. 单击可倒退
6. 单击可前进
7. 单击可跳至结束点
8. 单击可控制播放进度
9. 单击可调节音量

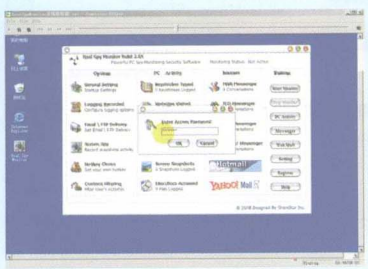
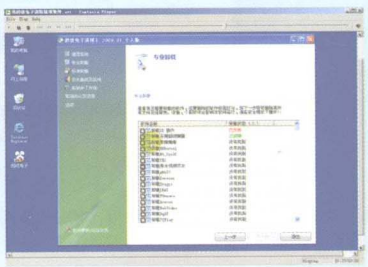
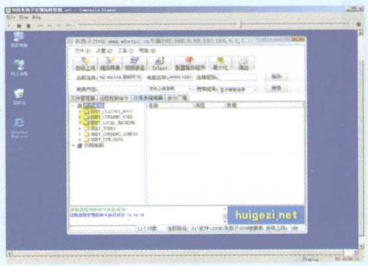
多媒体教程讲解演示



操作提示：

通常情况下，将配套光盘放入光驱后，多媒体教程会自动运行，并打开播放主界面。如果没有自动运行，可以通过双击光盘根目录下的AutoRun.exe来运行。

多媒体语音视频教程索引

前言

随着网络的普及，越来越多的人投入到网络生活中来，然而人们在享受便利网络的同时，还要时刻面临黑客攻击的危险。如果不了解入侵者的手段，没有及时采取必要的防御措施，一旦出现问题有可能造成很大损失。

出于安全及其他原因，传统教学往往只注重表面应用而避开一些敏感的技术。设想一下，如果一个网站的管理员只会架构网站，却不知黑客如何入侵网站，那如何会对自己网站的缺陷了如指掌？如何及时获知最新漏洞的描述信息而提前做好防御呢？

我们根据自己多年的亲身体验，在系统总结网络中广为使用的入侵、防御技术的基础上，针对黑客技术初学者、广大计算机安全技术爱好者以及网络管理人员编写了此书。希望能够帮助读者从黑客技术的角度了解网络安全技术，从而更有效地保护自己的计算机和网络安全。

本书以深入剖析入侵过程为主线来展开内容，向读者详细介绍了入侵者如何实现信息的搜集，如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵），如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日志防止目标服务器发现入侵痕迹。

此外，书中还详细介绍了入侵者是如何实现从信息扫描到入侵过程中的隐身保护。全书对每一个入侵步骤作了详细的分析，以推断入侵者在每一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的问题作必要的说明与解答，此外，还对几种常见的入侵手段进行了比较与分析。

另外，本书附带一张精心开发的专业级多媒体教学光盘，它采用全程语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式，紧密结合书中的内容对各个知识点进行深入的讲解，大大扩充了本书的知识范围。真正实现了以实例带动讲解、图例解说、面向应用的教学效果，便于初学者快速上手。

本书及配套的多媒体光盘主要面向黑客技术初学者、计算机安全技术爱好者及网络新手，强调实用、适用，可操作、能参考。

本书由众多经验丰富的网络安全技术专业人士编写，具体编写情况是：李防负责第1章，翟长霖负责第2章，段玲华负责第3章，陈艳艳负责第4章，刘伟霞负责第5章，张晓新负责第6章，孙世宁、田永燕负责第7章，杨平负责第8章，李伟、王英英负责第9章，

郑静、梁铎负责第10章，冯世雄负责附录部分，最后由武新华统审全稿。本书在编写过程中还得到了许多热心网友的支持，并参考了大量来自网络的资料，对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

由于作者水平有限，书中疏漏之处在所难免，恳请广大读者批评指正。

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计算机的行为都属于违法行为，希望读者在阅读本书后一定不要使用本书中介绍的黑客技术对他人计算机进行攻击，否则后果自负。

为便于读者阅读和理解，本书在写作中使用了如下图标约定：

对文章中所涉及到的一些内容进行特别描述，提醒读者注意操作到此处切忌犯的一些常识性错误。

提示读者关于文中所述内容的一些相关信息，以及对文中的重要内容作进一步阐述。

对实际操作中的一些小技巧进行阐述，告诉读者应该如何进行具体操作。

编者

2009.3.1

目 录

Chapter1 安全的测试环境：虚拟机

重点提示

- 使用VMware创建虚拟机
- 使用Virtual PC创建虚拟机
- 构建虚拟网站平台

导 读

随着 Internet 的普及，遭遇黑客的机会也越来越多，所以计算机使用者有必要了解和掌握一些黑客方面的知识，以便提高计算机的安全性能，防患于未然。

本章着重介绍了使用 VMware 和 Virtual PC 两款虚拟机工具为用户构建虚拟机的操作方法，从而在虚拟机中创建安全的测试环境，为学习黑客知识提供一个安全、有效的平台。

1.1 创建安全测试环境

所谓黑客原来是指那些精通计算机系统及网络技术的人，他们利用专业知识，出于娱乐爱好而热衷于编制新程序的人。但在今天，黑客经常会对系统进行修改或破坏，入侵别人的计算机，并可能会恶意地破坏计算机系统，取得利益，或只是为了显示自己的能力而制造计算机病毒。所以，现在黑客的确切定义是，在数据安全领域，未以授权、又企图躲过系统访问控制程序的检查而进入计算机网络的用户。

初步涉足黑客领域的学者，因在学习过程中需要找到符合条件的目标计算机进行模拟攻击，而这些目标计算机并不是能够从 Internet 上搜索到的，即使找到了目标计算机也不能随便进入，因为可能涉及法律问题，构建虚拟机是个很好的解决办法。

1.1.1 安全测试环境概述

所谓安全测试环境是指专门用于测试和学习黑客工具操作方法的实验平台，即在已存在的系统中，利用虚拟机创建一个内在的系统，该系统可以与外界独立，但与已经存在的系统建立网络关系，从而方便使用某些黑客工具进行模拟攻击，并且一旦黑客工具对虚拟机造成了破坏，也可以很快恢复，不会影响本来的计算机系统。

因需要使用黑客软件进行模拟攻击，所以创建虚拟机需满足如下条件：

- 尽量安装防御能力较差的系统，且不要安装其有关安全漏洞方面的补丁。如虚拟机中的系统为 Windows XP，则应安装其第一版本，且不要安装 SP1、SP2、SP3 及其后的有关补丁，以便于侦测和模拟攻击。
- 不要安装杀毒软件和防火墙。因为这些软件能够防止黑客工具的攻击和进入，会导致操作失败。
- 系统与软件运行的密码应为空，可以简化攻击时的麻烦。
- 根据所使用的黑客软件的功能和攻击对象的要求安装相应的软件，如 SQL Server 等。

自己的系统也不能安装杀毒软件和防火墙，否则黑客工具将不能在自己的系统中保存。

1.1.2 虚拟机软件概述

虚拟机（Virtual Machine）是指可以像真实机器一样运行程序的计算机的软件实现，是计算机科学体系中的一种特殊软件，它可以在计算机平台和终端用户之间建立一种环境，终端用户基于这个环境来操作软件。

根据运用方式和与直接机器的相关性，虚拟机可分为两大类，即系统虚拟机和进程虚拟机。系统虚拟机提供一个可以运行完整操作系统的系统平台。进程虚拟机可以运行单个计算机程序，支持单个进程。虚拟机的一个本质特点是，运行在虚拟机上的软件被局限在虚拟机提供的资源里——它不能超出虚拟世界。

虚拟机顾名思义就是虚拟出来的计算机，和真实的计算机几乎完全一样，区别是其硬盘是在