电脑报 总策划

就该这样入手

黄国耀 编著

黑客攻防

实战操作 全面剖析黑客攻防招式

扫描嗅探、木马植入、安全防范一本就够
病毒、黑客、网站、服务器攻防高手过招
1000余条黑客攻防技巧拿来就用

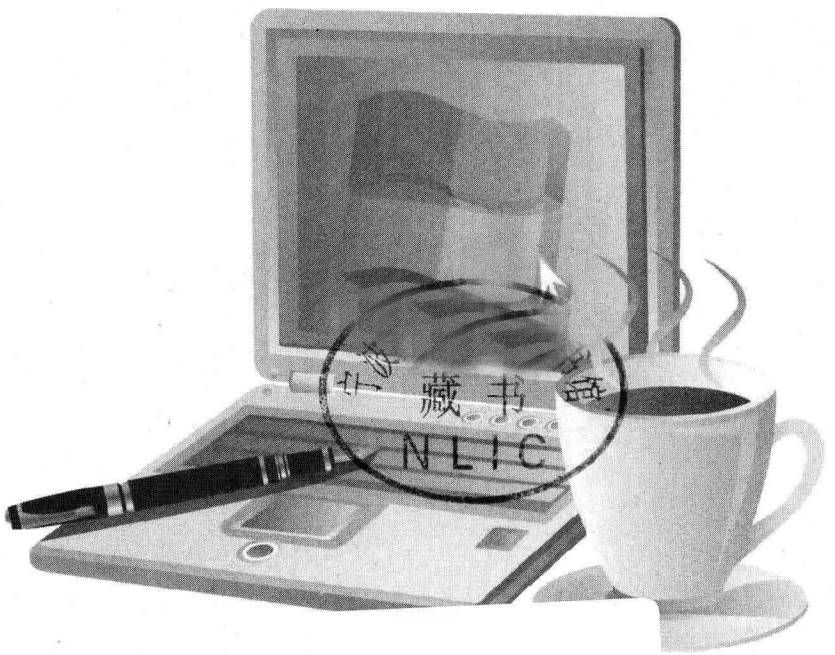
多媒体教学光盘
300分钟教学视频
电脑报精品电子书
丰富实用黑客攻防工具

超值赠送
金山毒霸2013

电脑报电子音像出版社
CPCW ELECTRONIC & AUDIOVISUAL PRESS

黑客攻防

黄国耀　编著



电脑报电子音像出版社
CPCW ELECTRONIC & AUDIOVISUAL PRESS

内容提要

本手册采用实例的形式为大家详细地剖析了黑客的攻防手段和攻防要领，同时给出了相应的防范方法。主要内容包括入侵前的信息搜集、软件攻防、常见密码攻防、病毒木马植入与防范、扫描嗅探、网络钓鱼与网页挂马、端口进程攻防、局域网与网吧攻防、网站与服务器攻防、远程监控等，涉及黑客攻防的方方面面，只要一本，就可以让你完全掌握黑客攻防技术。

本手册不仅可以作为初学者自学、培训时的参考用书，还可以作为对黑客、安全感兴趣的电脑爱好者的进阶指南。

光盘要目

1.手册配套视频教程

2.赠送《金山毒霸》杀毒软件

3.黑客攻防常用工具

4.《进程攻防实例解析》、《信息搜集与扫描》等电子书精选

黑客攻防

编　　著：黄国耀
责任编辑：李　勇
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
服务电话：(023)63658888-12031
发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：四川省蓥山数码科技文化发展有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：787mm×1092mm 1/16　17.5印张　250千字
版　　号：ISBN 978-7-89476-749-3
版　　次：2013年3月第1版　2013年3月第1次印刷
定　　价：35.00元（1CD+手册）

[本出版物所使用方正字体经方正授权许可]
[本出版物引用的商标或产品名称，其版权分别属于各注册公司]

学电脑，就该这样入手

●电脑报最新入门经典

●内容全、技术新，引领IT潮流

●资深电脑教学专家编写，充分尊重初学者认知规律

首先感谢您选择《就该这样入手》系列丛书，它是初学者的福音，更是读者电脑应用的好帮手。

作为电脑报精心组织编写的经典入门读物，《就该这样入手》系列丛书的策划、组稿和编辑工作前后长达一年。在广泛搜集了众多读者和教育专家的意见后，《就该这样入手》系列图书才得以完善编写方案，并在出版过程中得到了众多资深电脑教学专家的大力支持。

摆在读者朋友们面前的这套《就该这样入手》，主要具有以下五大特色：

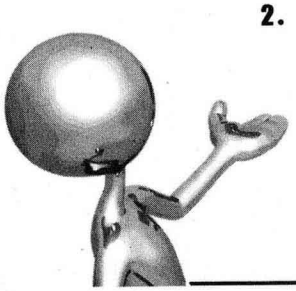
1. 任务式讲解，让电脑学习更有针对性

一般电脑图书大多是采用“第一章”、“第一节”的章节体系来组织图书内容，这样的框架体系相对比较系统，但是会讲很多大家根本就不必掌握的内容，从而让读者学习没有针对性，费时费力不说，还增大了学习的难度。

《就该这样入手》系列丛书则采用“讲”和“课”的任务式学习模式，让大家回到课堂教学“有的放矢”的学习方式，学习更有针对性，当然学习效率也就更高！

此外，在每一课还设置了“学习要点”、“动手练一练”、“常见问题解答”、“小知识”等内容，可以让大家在学习过程中提升动手操作能力，并最终做到融会贯通，从而学之能用，用之有效！

2. 多媒体光盘引导，手把手教您提升“战斗力”



对于很多初学者而言，最担心的就是电脑实战操作，总是难以克服这样那样的障碍，这其实就是实战经验不足或动手操作太少的缘故。该

系列提供了全程配套多媒体视频教学演示，读者既可以通过视频光盘边看边练，也可以在遇到问题的时候再看看教学视频上是如何操作的，从而真正有效提升自己的操作“战斗力”！

3．图文贴心编排，每本都可以独立作为一部操作“大全”使用

《就该这样入手》系列的每一分册都是该类别中的“小权威”，体现了“大全”的思路，凭此一本就可以从头开始完全掌握该类操作与应用。图书采用双栏编排方便阅读，图片添加的大量图解提示，可帮助直观理解和对照操作。新手上路，从入门到精通，一本就够！

4．买一送三，精彩电子书倾情回馈

为回馈读者，凡购买《就该这样入手》系列丛书，读者在光盘中都可以免费获得特别赠送的精美电子书。这些电子书都是本社在近期推出的一系列精品读物，包括网上开店、网络赚钱、黑客攻防等热门内容。

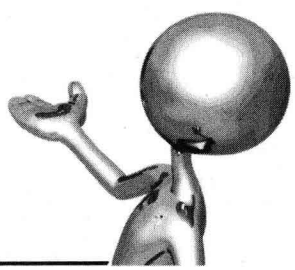
5．随光盘附赠超值杀毒软件，让电脑安全无忧

光盘中还特别赠送了《金山毒霸》杀毒软件，金山毒霸简易直观的用户界面、强大全面的安全防护功能将保护您和家人远离病毒入侵的威胁！

《就该这样入手》系列丛书不仅包含了电脑入门、五笔打字、电脑上网、办公应用等基础内容，还涵盖了黑客攻防、网络组建等热门专题。如果你是一位初学者，不妨按照课时安排循序渐进地学习；如果你具备一定的电脑基础，则可以跳过部分基础知识，直接学习提高篇的进阶应用。

最后，祝愿所有的读者都能在《就该这样入手》系列丛书的引导下轻松学习，快速成长为一名电脑应用高手！

编　者



第1讲 黑客入侵前的信息搜集

• 光盘配套多媒体视频教学：15分钟 •

当网络逐步普及，“黑客”这个词就逐步走入我们的生活，黑客并不遥远，你需要随时做好防范方能在复杂的网络环境中不被他人攻击！那么，黑客入侵前到底需要了解哪些信息才能发动攻击呢？在本讲中将首先为大家剖析黑客攻防中的信息搜集工作，这主要包括被攻击机器的操作系统、漏洞、端口开放情况等，而网络、QQ、博客等地方将很有可能成为黑客搜集信息的场所。

第2讲 微博、QQ与旺旺安全防范

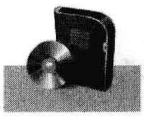
• 光盘配套多媒体视频教学：12分钟 •

本讲将进入黑客攻防的实际操作阶段，其中以QQ为首的聊天软件的安全自然是大家最为关心的。如今上网用户日益增多，而上网用户中，很多入门级的网虫，干得最多的事情就是上网聊天。正因为网上聊天的用户基数非常大，这也让黑客和伪黑客们对这个群体格外“关注”，于是QQ、旺旺就成了重灾区，甚至连最新的微博也难逃黑客们的“视线”，本讲将与大家一起揭露针对聊天软件的攻击手段，并介绍相应的防范方法。

第3讲 加密、解密与突破实例剖析

• 光盘配套多媒体视频教学：10分钟 •

提到密码，大家当然再熟悉不过了，如今生活、工作中密码无处不在，特别是当我们的生活与电脑、网络结合在一起的时候，你会发现没有密码可谓“寸步难行”：打开电脑要密码、登录QQ要密码、收发邮件要密码……然而，你的密码设置可靠吗？什么样的密码才安全？黑客常用哪些手段来破解密码，又该如何确保自己的电脑密码安全呢？下面将与大家一起探讨。



第4讲 局域网与网吧安全攻防

• 光盘配套多媒体视频教学：15分钟 •

局域网以其资源共享的优点赢得了众多单位、企业、网吧的厚爱，如今，很多家庭也组建了家庭局域网。的确，局域网资源分享非常快捷、方便，然而局域网方便的背后却也隐藏着巨大的隐患，同处局域网中，有着“近水楼台先得月”的优势，因此，针对局域网的攻击也就更为简单了。

第5讲 网络钓鱼与挂马攻防实例

• 光盘配套多媒体视频教学：12分钟 •

网络钓鱼和网页挂马是最近两年才兴起的网络攻击方式，其主要手段就是冒充一些正规的网站来骗取用户的信任，或者干脆就在正规网站中嵌入恶意攻击代码，让访问的用户中招，轻则感染病毒木马，重则直接盗取用户的密码、骗取钱财等，对此类攻击，大家应高度重视。

第6讲 进程与端口攻防实例

• 光盘配套多媒体视频教学：10分钟 •

Windows进程和端口是很多用户最容易忽略的，甚至有的新用户都不知道他们的存在，然而，进程和端口在系统安全中也起着非常重要的作用，黑客常常会利用系统开放的端口入侵你的电脑，因此，不是必须开启的端口应该尽量关闭。而黑客或者病毒恶意程序入侵你的电脑后，通常会在系统进程中有所体现，所以，把好进程关则可以很好地防范黑客和各种有害程序。

第7讲 常见漏洞攻防实例

• 光盘配套多媒体视频教学：15分钟 •

漏洞也称安全缺陷，不论是操作系统还是常用的工具软件，往往都存在一些安全漏洞。我们常听说需要给系统或者软件打补丁，正是这个原因。在编写操作系统代码时，由于考虑不周等原因造成的系统漏洞，属于先天不足，因此，它带来的后果一般都是致命的。系统漏洞攻击不管是黑客高手，还是骇客、菜鸟，都可以采而用之。而各种软件由于开发实力和精力有限，漏洞更是不少。下面就为大家介绍常见的漏洞攻击防范方法，并教会大家如何检测自己电脑系统的漏洞。

第8讲 黑客远程监控实例剖析

• 光盘配套多媒体视频教学：12分钟 •

远程控制一直是黑客非常感兴趣的东西，也是黑客攻防中非常关键的技术。控制与反控制历来就是黑客与安全人员之间的对抗，黑客总是想拿到掌控权，而安全人员则极力做好安全配置，以防范黑客进行控制，他们在不断的较量中相互制约。

第9讲 系统账户与口令攻防

系统安全是电脑安全中非常重要的一部分，很多攻击往往都起源于系统入口被攻破，所以，我们应特别重视系统账户和密码的安全。本讲中，将以当前主流的WinXP、Win7、Win8为例，分别介绍相应系统账户的破解、安全管理以及密码恢复等内容。

第10讲 网站与服务器攻防实例

• 光盘配套多媒体视频教学：10分钟 •

网站和服务器都是黑客最喜欢下手的对象，不过，由于网站和服务器都具有基本的保护措施，所以相对于一般上网的个人电脑而言显得较不易入侵成功。然而，由于很多服务器软件或操作系统的设计缺陷，常会造成各种各样的漏洞，因而让黑客们有机可乘，甚至造成网络灾难。在本讲中，将讨论黑客对网站和服务器的入侵及攻击流程，以及如何进行相应的防范。

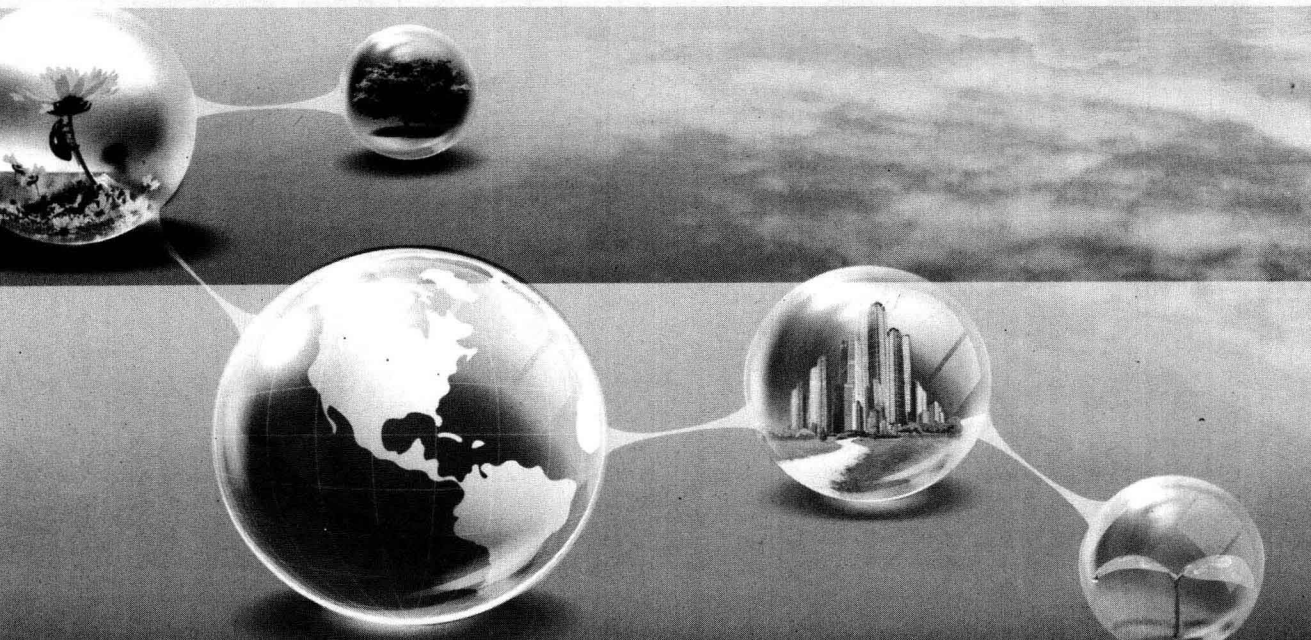
Chapter 01

第1讲 黑客入侵前的信息搜集

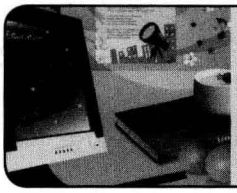
当网络逐步普及，“黑客”这个词就逐步走入我们的生活，黑客并不遥远，你需要随时做好防范方能在复杂的网络环境中不被他人攻击！那么，黑客入侵前到底需要了解哪些信息才能发动攻击呢？在本讲中将首先为大家剖析黑客攻防中的信息搜集工作，这主要包括被攻击机器的操作系统、漏洞、端口开放情况等，而网络、QQ、博客等地方将很有可能成为黑客搜集信息的场所。

本讲要点

- Google探测有漏洞的网站
- 认识黑客社会工程学
- 挖掘QQ、博客、QQ群中的信息
- 拒绝做“肉鸡”
- 隐藏IP增强安全
- 信息筛选的三种方法



第1课 操作系统和网站信息搜集



对一台电脑进行黑客攻击前，攻击者往往首先就要确定这台电脑使用的操作系统是什么。因为对于不同类型的操作系统，其上的系统漏洞有很大区别，那么黑客使用的方法就会完全不同。甚至，同一个操作系统，因为安装的SP补丁包版本不同，也直接关系到黑客任务的成败。而对网站的入侵更是如此。

1.1 搜集操作系统版本

要确定目标电脑正在使用的操作系统是什么，对于初入安防之门的读者来说，推荐使用下方的探测方法来获知。

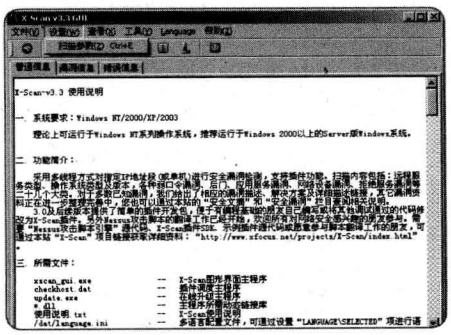
1.X-Scan介绍

X-Scan是一款功能比较全面的扫描器程序，扫描器是黑客兵器库中不可或缺的一部分，有了它的帮助，“黑客”们就会如虎添翼。扫描器不同于一些常见的攻击工具，它只能用来发现问题，而不能直接攻击目标机器，通过执行如下操作，可以完成远程电脑的操作系统探测。

2.探测步骤

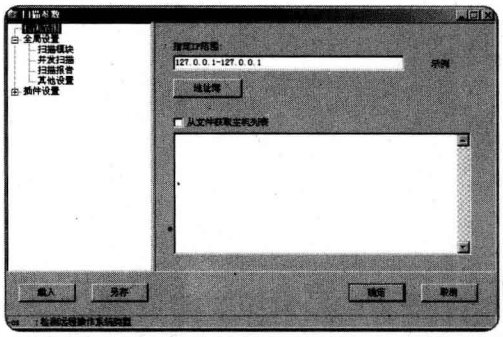
步骤01 首先，到国内著名的安全网站“安全焦点”（“http://www.xfocus.net/tools/200507/1057.html”）下载X-Scan v3.3 中文版。

步骤02 在完成下载并解压后，运行其中的“Xscan_gui.exe”打开如图所示的界面。



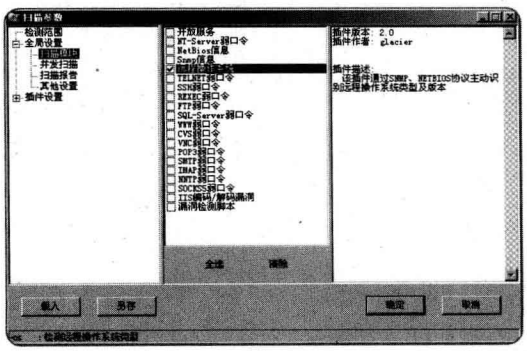
▲ Xscan软件

步骤03 依次单击“设置”→“扫描参数”菜单，在弹出的如图所示对话框中，在“检测范围”设置面板的“指定IP范围”栏中输入要扫描的目标电脑的IP地址。



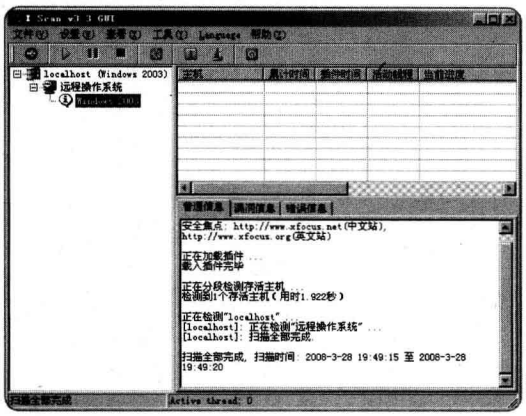
▲ 指定IP范围

步骤04 在“全局设置”→“扫描模块”设置界面中勾选“远程操作系统”项，通过右侧的说明，可以看出远程电脑的操作系统识别是通过“SNMP、NETBIOS协议主动识别远程操作系统类型及版本”插件来完成的，如图所示。



▲ 扫描参数

步骤05 在单击“确定”按钮返回到“Xscan_gui.exe”主窗口后，单击“开始扫描”按钮后，耐心等待片刻就可以看到如图所示的扫描结果了。



▲ 扫描结果

步骤06 在左侧的扫描目标右侧可以看到“Windows 2003”的标识，这告诉我们这是一台正在使用Windows 2003的电脑，进而可以分析出这台电脑可能是台服务器，理由很简单：个人电脑一般只会安装Windows XP或Vista。

3.通过网站判断

有时，黑客会通过网站来获得目标的操作系统信息，例举：

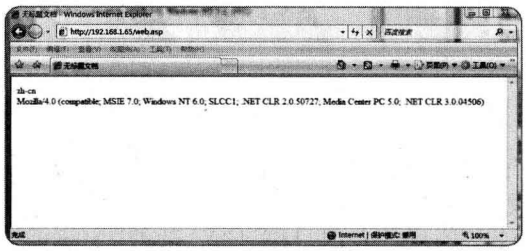
某黑客与某个人电脑用户通过 QQ 聊天，黑客说：“我的网站不错，欢迎你来访问。”，并给出一个网页地址。很多个人电脑用户不会提防这个要求，于是立即访问了这个网页。

在访问这个网页的同时，此个人电脑用户的操作系统信息实际上已经被写入到了数据库中了。这样，黑客不费吹灰之力就得到了想要的信息。

这样的获取指定信息的代码很简单，实现的方法有很多。比方说，下面的代码就可以在网页上显示客户端的操作系统等信息。

```
<%
Response.write ? Request.ServerVariables("HTTP_ACCEPT_LANGUAGE") & "<br>" Response.write ? Request.ServerVariables("HTTP_USER_AGENT") & "<br>"
%>
```

在访问含有上述代码的网页时，会看到如图所示的信息显示。通过这些信息，可以知道个人电脑用户的 IE 版本、操作系统版本，等等。这些信息都可以用于黑客任务。



▲ 网站获取信息

上述方法是使用了服务器变量集合保存了随 HTTP 头请求一起传送的 HTTP 头的信息，HTTP 头中包含有很多来访者（客户端）的信息，可以通过它获得有关来访问者操作系统版本、浏览器版本等信息。

1.2 Google探测有漏洞的网站

随着 Internet 的飞速发展，面对海量而又不断更新的信息库，如何快速准确地找到自己需要的信息已经变得越来越重要了。为了使网民搜索信息的速度更加快捷、准确，专门在 Internet 上执行信息搜索任务的搜索引擎技术应用而生了。目前，网络中使用率最高的搜索引擎是 www.google.com，如图所示。

▲ Google搜索

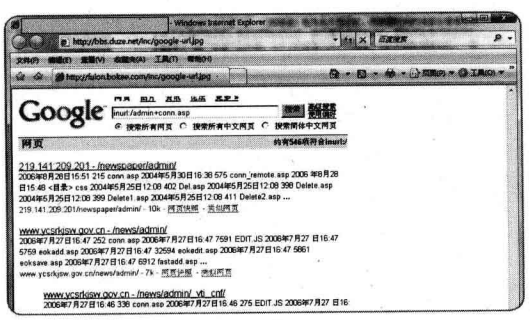
面对互联网上仅次于邮件的第二大互联网应用——搜索引擎，黑客都是怎样利用它的呢？搜索引擎对于入侵的帮助是不可或缺的，它可以帮助我们快速找到漏洞的资料、工具的下载路径、攻击的方法、存在漏洞的网站，等等。

1.搜索特殊的“关键词”

通过搜索引擎网站，黑客可以通过搜索特殊的“关键词”来查找到一些具有漏洞的网站。比方说，在动态网站中一般会有CONN.ASP这个文件，它用于存储数据库文件的路径、名称等信息。显然，这个文件是非常重要的，所以，黑客在搜索引擎中总是喜欢使用它做为搜索关键词，如：

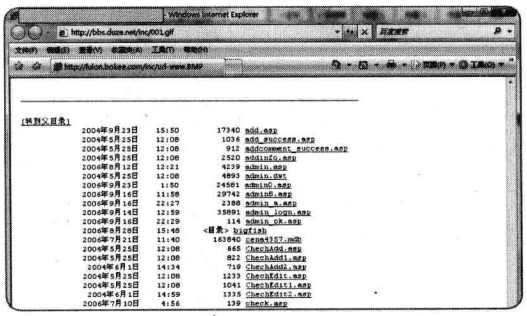
inurl:/admin+conn.asp

其中，admin表示后台管理目录，它通常用于存储所有的管理文件。当然，也可以改成一些其它的目录名，但目录名要在网站中存在才行，如图所示。



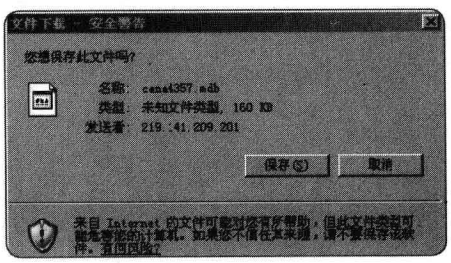
▲ 搜索关键词

在单击第一个搜索结果后，将会打开如图所示的页面，在这里可以看到这个网站的管理结构。



▲ 网站的管理结构

其中，甚至可以看到存储网站内容（如管理员用户名和密码）的数据库文件（后缀名为mdb），在单击此文件后，可以立即把它下载到当前电脑中，如图所示。



▲ 数据库文件

在使用Access 2007等软件打开此数据库文件后，就可以获得网站各种重要的信息了，此时，网站的管理权限已经意味着被黑客得手了。

提 示

在www.google.com中黑客使用的关键词有很多，如upload.asp site:tw、inurl:winnt\system32\inetsrv\等，这些关键词都可以为黑客起到为虎作伥的作用。

2.Google Hacker威力无穷

当搜索引擎的强大“入侵”功能让黑客着迷时，各种各样可以利用搜索引擎来实施黑客任务的工具就层出不穷了。下面，就以实例