电脑报 总策划

黑客

入门与成长 秘技108招

步步為營

实例·上手篇

黄国耀 编著

实例剖析
黑客入门
攻防招式
全程实战

信息搜集让你“无处藏身”
QQ被盗、心中永远的痛
当心“藏污纳垢”的进程
看好你的大门—端口
永远的特洛伊木马
网络扫描、嗅探与监听
网吧黑客的反击
网络钓鱼与网页挂马
黑客最青睐的“漏洞”
深入浅出玩转网站攻防

精彩光盘

- 正版可牛杀毒软件
- 黑客攻防视频教程
- 杀毒反黑与漏洞检测工具
- 加密解密与远程控制工具
- 十大黑客电影赏析

电脑报电子音像出版社
CPCW Electronic & Audiovisual Press

黑白棋

入门与成长

秘技108招

步步為營

实例·上手篇

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剖析了黑客入门与成长必备的攻防技能，内容包括：信息搜集让你“无处藏身”、QQ攻击与防范、当心“藏污纳垢”的进程、看好系统端口、永远的特洛伊木马、网络嗅探与监听、网吧黑客的反击、网络钓鱼与网页挂马、黑客最青睐的“漏洞”、深入浅出玩转网站攻防、反侦查的电脑安全铁律等。内容涵盖了黑客攻防的方方面面，而且以全程实战的方式为大家讲解，可以让大家轻松掌握黑客从入门到精通的攻防要领。

光盘要目

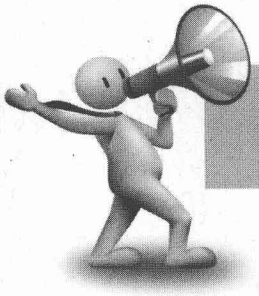
- 正版可牛杀毒软件
- 杀毒反黑与漏洞检测工具
- 十大黑客电影赏析
- 黑客攻防视频教程
- 加密解密与远程控制工具

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法用途，后果自负。

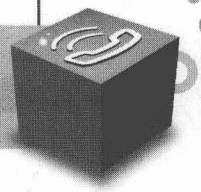
黑客入门与成长秘技108招

编　　者：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：重庆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有限公司
文本印刷：重庆市联谊印务有限公司
开本规格：787mm×1092mm 1/16　18印张　200千字
版　　号：ISBN 978-7-89476-482-9
版　　次：2010年10月第1版 2010年10月第1次印刷
定　　价：35.00元(1CD+手册)

前言



揭秘黑客谋略与兵器精髓



这是一套全面指导黑客入门与实战的黑客图书
这是一套深刻解析攻防工具及应用的黑客图书
这是一套完全精通攻防谋略与技巧案例的黑客图书

网络就是战场、安全就是用兵。

战场上硝烟弥漫，鲜血迸溅；网络中针锋相对，明争暗斗！

黑客世界的刀光剑影总让人感到神秘莫测。

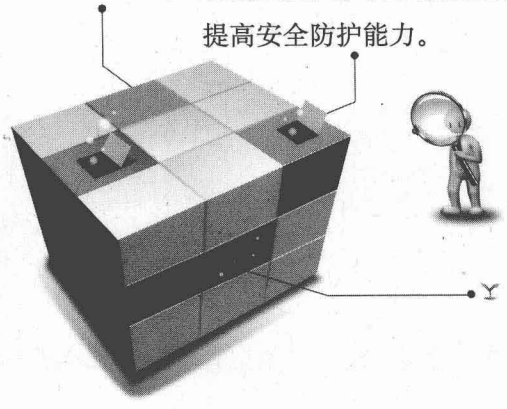
正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

一名技艺高超的黑客无非体现在以下三方面：其一是掌握常见的黑客攻防手法，其二是娴熟的黑客工具应用，其三是独到的谋略技巧施展。本系列图书正是围绕以上三方面的黑客攻防必备技能为读者全面展开并详细解读。

《黑客入门与成长秘技 108 招》：通过 108 招攻防技巧，由浅入深地为大家讲解了黑客成长必备的技能，让大家快速步入黑客之门。

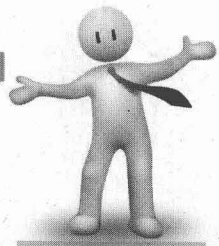
《黑客 88 种兵器全解析》：精选了黑客最常用的 88 种攻防工具，通过工具的实战操作帮助读者快速领悟黑客攻防手段。

《黑客攻防 36 计》：剖析了与黑客斗智斗勇的 36 个实战案例，全面解析黑客攻击过程，详尽介绍防范操作步骤，帮助你快速掌握黑客攻防的深度谋略与技巧，提高安全防护能力。



编 者

2010 年 10 月



光盘精彩导航

实用功能

本光盘可自启动电脑，并进入 Windows PE 系统，进行系统维护、杀毒等。还可通过 Ghost 软件进行系统一键备份，系统还原等操作。该光盘功能完善、实用，是你维护电脑的随身宝典。

正版可牛杀毒软件

可牛免费杀毒集成全球领先的卡巴斯基杀毒引擎、自主研发的高效轻巧云引擎，双剑合璧，完美清除木马病毒；首创双杀软模式，兼容其它杀毒软件；“浏览器医生”一键解决浏览器被篡改、桌面图标异常、恶意插件泛滥等问题，全面保障上网安全；快速智能的修复漏洞功能，与三种实时保护模式的结合，从根源上关闭病毒入侵的大门，为你提供全方位的安全保护。

杀毒反黑与漏洞检测工具

360 顽固木马专杀大全
Windows 系统漏洞扫描专家
超级巡警漏洞检测
光华系统漏洞修复工具
绿鹰 PC 万能精灵
微点主动防御软件
迅雷系统漏洞修复工具
墨者安全专家第二代 (防盗号版)
……

加密解密工具

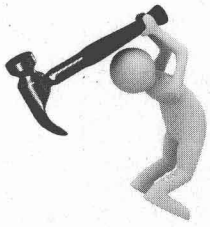
Passbay自由行密码管理软件
文件隐藏大师
加密奇兵
加密金刚锁
高强度文件夹加密大师
便携式文件夹加密器
Dekart Private Disk
……

系统安全辅助工具

肉鸡检测器
QQ医生
QQ聊天记录查看器
Windows流氓软件清理大师
360恶意网站屏蔽器
360时间保护器
黄山IE修复专家
江民网页安全专家
网络保镖
金山网盾
超级巡警之机器狗专杀
畅游巡警
……

十大黑客电影赏析

《战争游戏》（WarGames）
《通天神偷》（Sneakers）
《天才除草人》（The Lawnmower Man）
《网络惊魂》（The Net）
《黑客》（Hackers）
《杀人硬件》（Virtuosity）
《约翰尼记忆术》（Johnny Mnemonic）
《异次元黑客》（The Thirteenth Floor）
《黑客帝国》（The Matrix）
《剑鱼行动》（Swordfish）

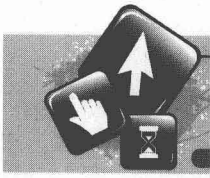


目录 CONTENTS

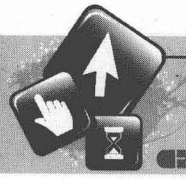
步步为营
黑客入门与成长秘技108招

第1章 信息搜集让你“无处藏身”

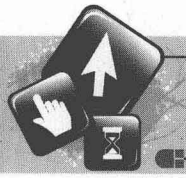
第2章 QQ被盗，心中永远的痛



第3章 当心“藏污纳垢”的进程

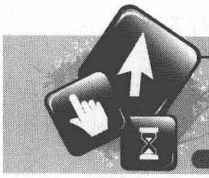


第4章 看好你的大门——端口

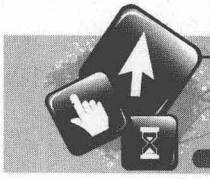


第5章 与病毒过招

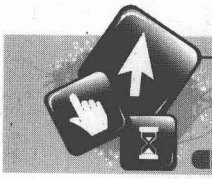
第6章 永远的特洛伊



第7章 网络扫描、嗅探与监听

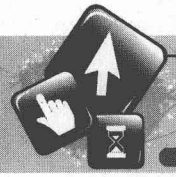


第8章 网吧黑客的反击

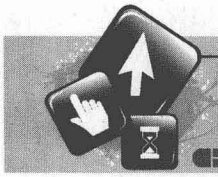


第9章 亦正亦邪的“远程控制”

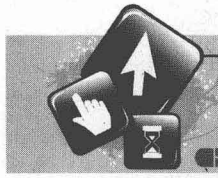
第10章 网络钓鱼与网页挂马



第11章 黑客最青睐的“漏洞”



第12章 深入浅出玩转网站攻防



第13章 反侦查的电脑安全铁律

第1章 信息搜集让你“无处藏身”

在黑客攻防中，信息搜集是一项非常重要的工作：从攻的角度看，需要了解被攻击机器的操作系统、漏洞情况、端口开放情况等；而从防的角度看，我们必须隐藏好自己的电脑相关信息，比如IP地址、个人QQ、甚至包括博客信息等。本章将为大家一一剖析信息搜集与防范要领。

第1招 用X-scan搜集系统版本信息

对一台电脑进行黑客行为，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，其系统漏洞有很大的区别，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，也会导致黑客任务的成败与否。

一、X-Scan介绍

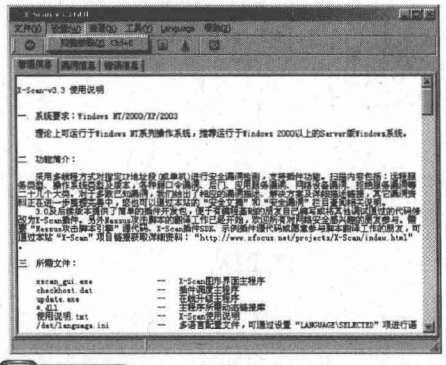
要确定目标电脑正在使用的操作系统是什么，对于初入安防之门的读者来说，推荐使用X-Scan来获知。

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，通过执行如下探测步骤，可以完成远程电脑的操作系统探测。

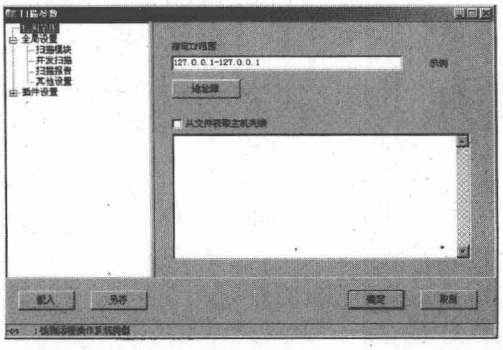
二、探测实战

步骤1 首先，至国内的著名安全网站“安全焦点”“http://www.xfocus.net/tools/200507/1057.html”下载X-Scan v3.3中文版。

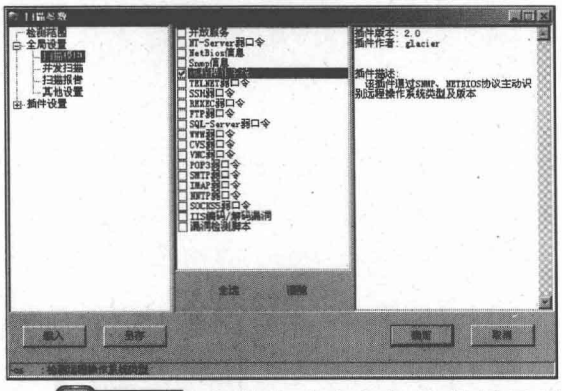
步骤2 在完成下载并解压后，运行其中的“Xscan_gui.exe”打开如图所示的界面。



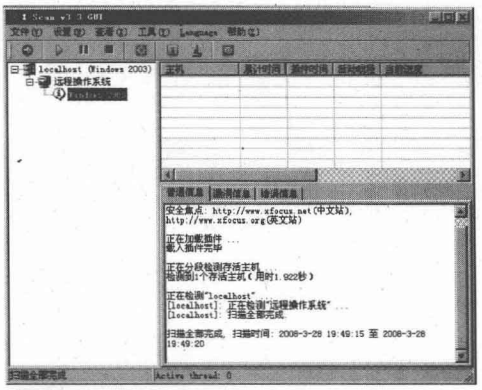
步骤3 依次单击“设置”→“扫描参数”菜单，在弹出的如图所示对话框中，在“检测范围”设置面板的“指定IP范围”栏中输入要扫描的目标电脑的IP地址。



步骤 4 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。



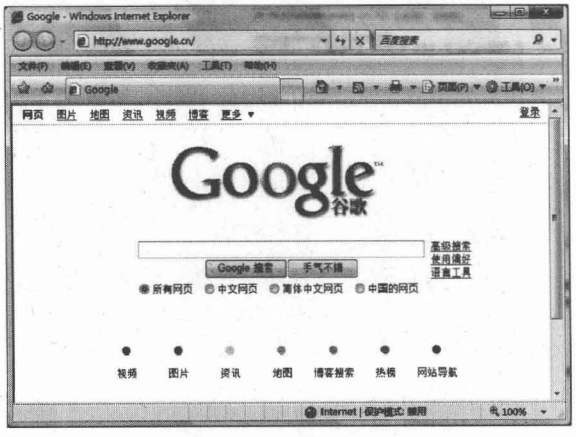
步骤 5 在单击“确定”按钮返回到“Xscan_gui.exe”主窗口后，单击“开始扫描”按钮后，耐心等待片刻就可以看到如图所示的扫描结果了。



步骤6 在左侧的扫描目标栏中可以看到“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。

第2招 Google竟成黑客“帮凶”

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运而生。目前，网络中使用率最高的搜索引擎是 www.google.com，如图所示。



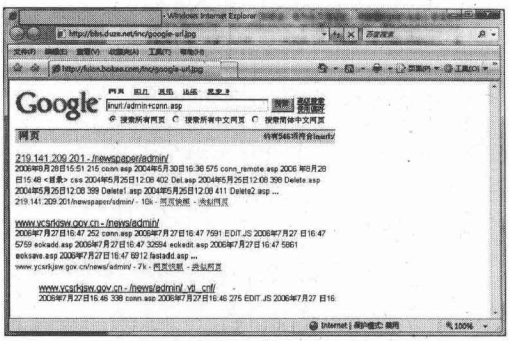
面对互联网上仅次于邮件的第二大互联网应用——搜索引擎，黑客都是怎样利用它的呢？搜索引擎对于入侵的帮助是不可或缺的，它可以帮助我们快速找到漏洞的资料、工具的下载路径、攻击的方法、存在漏洞的网站，等等。

一、搜索特殊的“关键词”

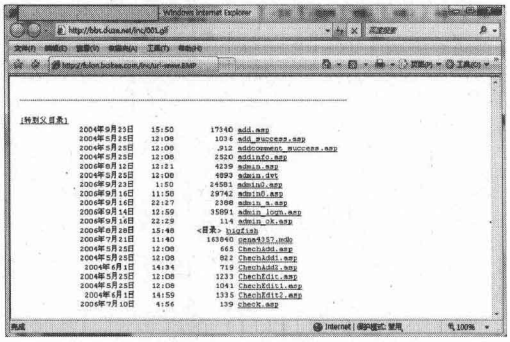
通过搜索引擎网站，黑客可以通过搜索特殊的“关键词”来查找到一些具有漏洞的网站。比方说，在动态网站中一般会有 CONN.ASP 这个文件，它用于存储数据库文件的路径、名称等信息。显然，这个文件是非常重要的，所以，黑客在搜索引擎中总是喜欢使用它作为搜索关键词，如：

inurl:/admin+conn.asp

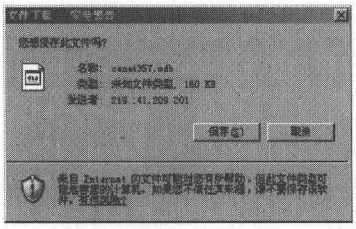
其中，admin 表示后台管理目录，它通常用于存储所有的管理文件。当然，也可以改成一些其他的目录名，但目录名要在网站中存在才行，如图所示。



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。



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。



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 ATTENTION

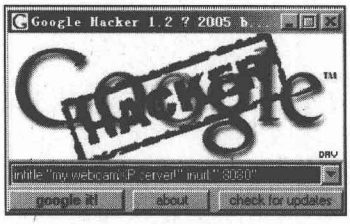
在 www.google.com 中黑客使用的关键词有很多，如 upload.asp site:tw、inurl:winnt\system32\inetsrv\ 等，这些关键词都可以为黑客起到为虎作伥的作用。

二、Google Hacker威力无穷

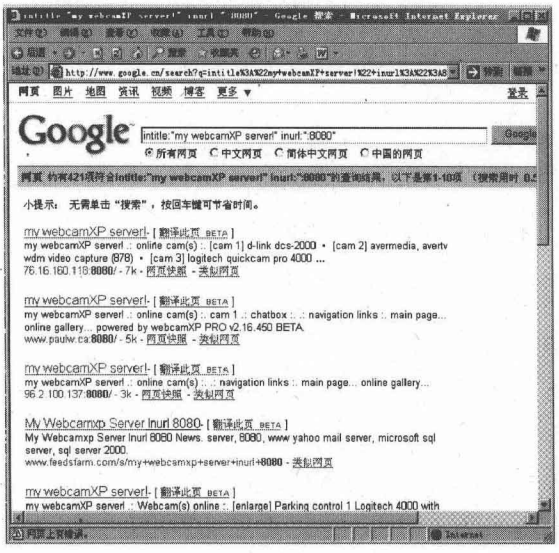
当搜索引擎的强大“入侵”功能让黑客着迷时，各种各样可以利用搜索引擎来进行黑客任务的工具就层出不穷了。下面，就以实例的方法为读者们演示一下“Google Hacker”的使用过程。为此，需要执行如下操作：

首先，至 http://winxppro.ys168.com/ 下载“Google Hacker 1.2”。

接着，在“关键词”列表中选择一个关键词，并单击“Google it”按钮继续，如图所示。



随即，将会打开 IE 浏览器访问 www.goole.com，并会自动输入指定的关键词进行搜索，如图所示。



提示 ATTENTION

由于列举的关键词都是常见的漏洞，所以搜索结果的数量通常都会比较惊人。

第3招 借助Ping命令和网站信息探测

一、使用Ping命令探测

Ping 命令是测试网络连接、信息发送和接收状况的实用型工具，这是一个系统内置的探测工具。

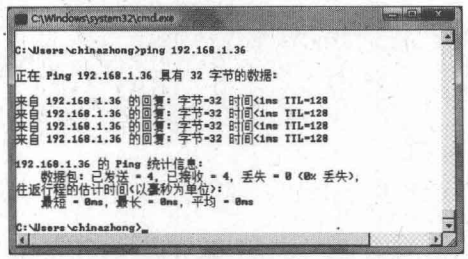
此命令的参数作用解释如下：

－t：不断使用 Ping 命令发送回响请求信息到目的地。要中断并退出 Ping，只需按“Ctrl+C”键。初级黑客常喜欢使用这个参数对目标电脑进行攻击。

－a：指定对目的地 IP 地址进行反向名称解析。如果解析成功，Ping 将显示相应的主机名。

－n Count：指定发送回响请求消息的次数，默认值为 4。

－l Size：指定发送的回响请求消息中“数据”字段的长度(以字节表示)。默认值为32，如图所示。size 的最大值是 65,527。



－f：指定发送的回响请求消息带有“不要拆分”标志（所在的 IP 标题设为 1）。回响请求消息不能由目的地路径上的路由器进行拆分。该参数可用于检测并解决“路径最大传输单位 (PMTU)”的故障。

－i TTL：指定发送回响请求消息的 IP 标题中的 TTL 字段值。其默认值是主机的默认 TTL 值。对于 Windows XP 主机，该值一般是 128，TTL 的最大值是 255。

－v TOS：指定发送回响请求消息的 IP 标题中的“服务类型 (TOS)”字段值。默认值是 0。TOS 被指定为 0 到 255 的十进制数。

－r Count：指定 IP 标题中的“记录路由”选项用于记录由回响请求消息和相应的回响应答消息使用的路径。路径中的每个跃点都使用“记录路由”选项中的一个值。如果可能，可以指定一个等于或大于来源和目的地之间跃点数的 Count。Count 的最小值必须为 1，最大值为 9。

－s Count：指定 IP 标题中的“Internet 时间戳”选项用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。Count 的最小值必须为 1，最大值为 4。

－j Path：指定回响请求消息，使用带有 HostList 指定的中间目的地集的 IP 标题中的“稀疏资源路由”选项。可以由一个或多个具有松散源路由的路由器分隔连续中间的目的地。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）。

－k HostList：指定回响请求消息，使用带有 HostList 指定的中间目的地集的 IP 标题中的“严格来源路由”选项。使用严格来源路由，下一个中间目的地必需是直接可达的（必需是路由器接口上的邻居）。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址(带点的十进制符号)。

－w Timeout：指定等待回响应答消息响应的时间（以微妙计），该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示“请求超时”的错误消息。默认的超时时间为 4000（4 秒）。

Target Name：指定目的端，它既可以是 IP 地址，也可以是主机名。

下面给出一些 Ping 命令的典型使用方法。

实例1：检测本机

要检测本机的网卡驱动程序及 TCP/IP 协议是否正常，只需在“命令提示符”窗口中输入“Ping 127.0.0.1”命令即可。由于 127.0.0.1 这个保留的 IP 地址指向到本机，所以可以通过此命令来检查本机的网卡驱动。

实例2：多参数合用检测

假设，现在使用“Ping a －t 202.102.