

黑客入门与成长

秘技100招

实例·上手篇

黄国耀 编著

步步
为营



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

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

实例剖析
黑客入门
攻防招式
全程实战

黑 夜

入门与成长 秘技100招

实例·上手篇

黄国耀 编著

步步
为营



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

版权所有 盗版必究

未经许可 不得以任何形式和手段复制和抄袭

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

C D 生产：四川省荃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

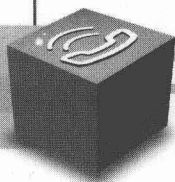
版 次：2010年10月第1版 2010年10月第1次印刷

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。

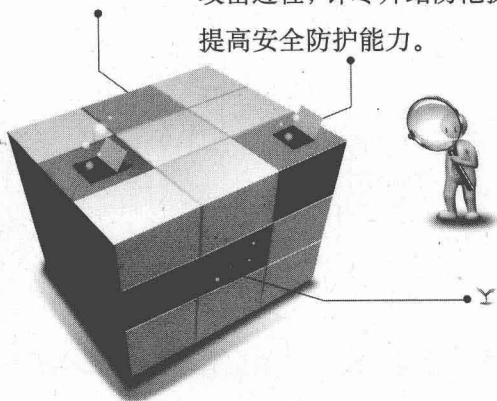
正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

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。

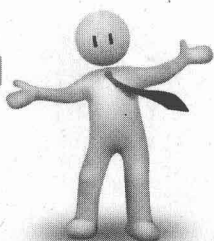
《黑客 88 种兵器全解析》：精选了黑客最常用的 88 种攻防工具，通过工具的实战操作帮助读者快速领悟黑客攻防手段。

《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

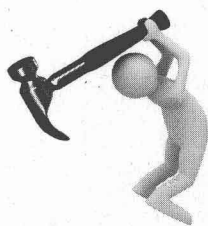
Passbay自由行密码管理软件
文件隐藏大师
加密奇兵
加密金刚锁
高强度文件夹加密大师
便携式文件夹加密器
Dekart Private Disk
.....

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1招 用X-scan搜集系统版本信息 ……001

- 一、X-Scan介绍 ……001
- 二、探测实战 ……001

第2招 Google竟成黑客“帮凶” ……002

- 一、搜索特殊的“关键词” ……002
- 二、Google Hacker威力无穷 ……003

第3招 借助Ping命令和网站信息探测 004

- 一、使用Ping命令探测 ……004
- 二、通过网站判断 ……005

第4招 网站：信息泄密的罪魁祸首 ……006

- 一、域名基础知识 ……006
- 二、探测域名与IP ……007
- 三、Nslookup命令查询IP信息 ……008
- 四、获得网站基本信息资料 ……008
- 五、查看网站备案登记信息 ……009
- 六、查看网站其它信息 ……010

第5招 迂回战术 认识黑客社会工程学攻防010

- 一、什么是社会工程学 ……010
- 二、黑客社会工程学的常用手段 ……011

第6招 QQ、博客，就这样被你出卖 ……012

- 一、挖掘你需要的QQ号 ……012
- 二、通过博客挖掘更多信息 ……013
- 三、从QQ开始“探路” ……013
- 四、不容忽视的QQ群 ……014

第7招 去伪存真 信息筛选有诀窍 ……015

- 一、人工筛选信息 ……015
- 二、软件筛选信息 ……017

第8招 隐藏IP增强安全 ……018

- 一、为什么要隐藏IP ……018
- 二、使用代理藏IP ……019
- 三、用提供匿名冲浪的网站隐藏IP ……019
- 四、Telnet入侵时隐藏IP ……020
- 五、使用工具软件藏IP ……020
- 六、验证IP是否隐藏成功 ……020

第9招 信息安全保卫战 拒绝做“肉鸡” 021

- 一、什么是“肉鸡” ……021
- 二、如何判断电脑是否为“肉鸡” ……021
- 三、使用软件检测是否为“肉鸡” ……022



第2章 QQ被盗，心中永远的痛

第1招 解析收文件QQ被盗的骗局 ……024

- 一、盗号骗局再现 ……024
- 二、双格式文件实例解析 ……024
- 三、防盗技巧 ……025

第2招 当心“QQ靓号”诱惑你 ……025

- 一、“QQ靓号”的诱惑 ……025
- 二、安全防范技巧 ……026

第3招 QQ强制视频聊天027

- 一、强制视频聊天解析 027
- 二、防范技巧 027

第4招 QQ聊天记录攻防027

- 一、聊天记录防范 027
- 二、强行聊天防范 029

第5招 爱Q大盗 使用邮箱就能盗029

- 一、配置QQ木马 029
- 二、突破软件的限制 030
- 三、运行木马 030

第6招 QQ申诉也被黑客利用031

- 一、木马客户端制作解析 031
- 二、QQ密码很容易被盗 031
- 三、QQ申诉信息“夺取”QQ号 032
- 四、防范技巧 032

第7招 巧施妙招 看好Q币、QQ通讯录 033

- 一、为QQ硬盘设置密码 033
- 二、为QQ通讯录设置密码 033

- 三、看好你的Q币 033
- 四、防骗技巧 034

第8招 巧用邮箱聊天 揪出隐身QQ好友 034

- 一、邮箱聊天揪出隐身好友 034
- 二、注意事项 035

第9招 借你一双慧眼 识破QQ骗局036

- 一、似是而非的QQ系统消息 036
- 二、“最新刷Q币”的骗局 036
- 三、“QQ防骗技巧”暗藏新骗局 038

第10招 使用密保卡保护QQ039

- 一、认识密保卡 039
- 二、QQ密保卡使用方法 040

第11招 为QQ保驾护航——QQ医生042

- 一、与诺顿联手，免费杀毒 042
- 二、系统漏洞扫描，安全可靠 042
- 三、下载限速，流量实时监控 042
- 四、木马扫描 043



第3章 当心“藏污纳垢”的进程

第1招 通通透透 认识Windows进程044

- 一、关闭进程和重建进程 044
- 二、查看进程的发起程序 045

第2招 自己动手 关闭恶意进程046

- 一、关闭任务管理器杀不了的进程 046
- 二、查看隐藏进程和远程进程 046
- 三、杀死病毒进程 047

第3招 当心藏污纳垢的SVCHOST.EXE进程048

- 一、SVCHOST.EXE是何物 048
- 二、识别SVCHOST.EXE中的病毒 048

第4招 真假李逵 Explorer.exe进程要认清049

- 一、什么是Explorer.exe进程 049
- 二、Explorer.exe容易被冒充 049

第5招 强力助手 Windows 进程管理器 050

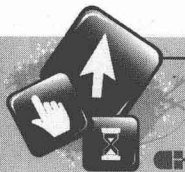
- 一、进程管理 050
- 二、恶意进程分析 051

第6招 超级巡警为系统进程护航051

- 一、全面查杀 051
- 二、实时防护 052
- 三、保险箱 052
- 四、系统安全增强工具 052
- 五、用SSDT工具清除流氓软件 053

第7招 堪比兵刃的超强手工杀毒辅助工具 054

- 一、从进程中发现可疑文件 054
- 二、查看网络端口与IE插件 055
- 三、强大的文件管理功能 055
- 四、服务与启动项管理 055



第4章 看好你的大门——端口

第1招 从零开始 认识系统端口057

- 一、什么是端口057
- 二、端口的分类057

第2招 熟能生巧 掌握端口基本操作 ...058

- 一、开启和关闭端口058
- 二、端口查看工具059
- 三、重定向本机默认端口059

第3招 3389端口入侵与防范060

- 一、什么是3389端口060
- 二、3389入侵实例剖析061
- 三、3389端口安全防范061

第4招 创建安全策略 过滤与禁止135端口 062

- 一、创建IP筛选器和筛选器操作062

- 二、创建IP安全策略063
- 三、指派和应用IPsec安全策略064

第5招 确保电脑安全 端口扫描利器不可少 064

- 一、常见端口剖析064
- 二、用SuperScan扫描端口安全065
- 三、NetBrute Scanner扫描端口066

第6招 多种手段保护Windows服务安全 067

- 一、什么是系统服务067
- 二、关闭无用服务保系统安全068
- 三、使用软件监控系统服务069

第7招 切勿乱动 系统“服务”权限设置有讲究 070

- 一、安全权限管理070
- 二、登录权限设置072



第5章 与病毒过招

第1招 入门必备 了解计算机病毒及其分类 073

- 一、计算机病毒的概念073
- 二、计算机病毒的分类073
- 三、计算机病毒传播途径073

第2招 简单可行 识破日常操作中的病毒文件 074

- 一、抵制下载软件中的“诱惑”074
- 二、识别邮箱中的“附属品”075

第3招 有的放矢 防范邮件附件病毒 ...075

- 一、什么是邮件附件病毒075
- 二、邮件病毒的“三大迷招”076
- 三、全面阻截邮件病毒078

第4招 胸有成竹 遭遇病毒时的应急措施 080

- 一、病毒发作实例演示080
- 二、遭遇病毒时的应急措施080
- 三、病毒防范要点082

第5招 搭建虚拟机 深入理解病毒发作 084

- 一、了解VMWare Workstation084
- 二、VMware Workstation的安装084
- 三、打造自己的虚拟计算机084
- 四、文件共享087
- 五、虚拟机中的木马实战088

第6招 影子系统 打造系统不破之身 ...090

- 一、什么是影子系统090
- 二、影子系统的特点090
- 三、影子系统PowerShadow091

- 四、数据保护伞ShadowUser 091
- 五、Returnil虚拟影子系统 093

第7招 免费“卡巴斯基”可牛双管齐下杀病毒093

- 一、联手卡巴斯基杀病毒 093
- 二、实时防护，给你全方位保护 094
- 三、高级防御，网页、邮件齐监控 095

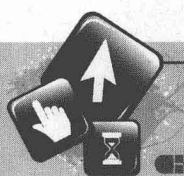
第8招 不用工具 命令行轻松反病毒 ...096

- 一、Tasklist揪出可疑进程 096

- 二、Ntsd结束病毒进程 096
- 三、Netstat查看开放端口 097
- 四、Find查看文件是否被捆绑 097
- 五、FC检查注册表是否被篡改 097

第9招 拒绝病毒 送你一把“保护伞” 098

- 一、自动更新病毒库 098
- 二、强大的病毒查杀能力 098
- 三、出色的实时防护 099



第6章 永远的特洛伊

第1招 木马的分类和结构 100

- 一、什么是木马 100
- 二、木马的分类 100
- 三、木马的结构 101

第2招 剖析常见木马入侵手法 101

- 一、木马入侵途径分析 101
- 二、木马的运行原理 102
- 三、木马隐形位置 103

第3招 影片木马攻击与防范 105

- 一、木马的起源 105
- 二、影片木马制作 105
- 三、影片木马安全防范 108

第4招 三招两式 围剿潜藏在RMVB中的木马 110

- 一、巧用RM恶意广告清除器 110
- 二、使用快乐影音播放器清除广告 110
- 三、迅雷也能查杀弹窗广告 111

第5招 防不胜防 听歌也会中木马 111

- 一、MP3中挂木马的原理 111
- 二、添加音乐文件 111
- 三、设置弹窗方式和弹出时间 112

- 四、设置木马网页地址并完成配置 112
- 五、MP3音乐“木马”防范措施 113

第6招 妙用冰河陷阱防冰河 113

- 一、冰河陷阱简介 113
- 二、清除冰河木马 114
- 三、诱骗骇客 114

第7招 揭秘图片病毒/木马的制作原理 116

- 一、什么是图片病毒 116
- 二、图片病毒的传播方式和原理 116

第8招 图片病毒与图片网马实战解析 ... 119

- 一、超强免杀图片病毒揭秘 119
- 二、图片网马实战解析 122

第9招 辨证施治 如何防范图片病毒 ... 124

- 一、安装补丁 124
- 二、安装杀毒软件 126
- 三、使用图片病毒专杀工具 126

第10招 巧借工具 识破木马的“马甲” 126

- 一、什么是木马的马甲 126
- 二、木马加壳实战 127
- 三、让加壳木马“脱壳” 127



第7章 网络扫描、嗅探与监听

第1招 Sss扫描器扫描实战129

- 一、什么是扫描 129
- 二、扫描实战 129

第2招 流光扫描弱口令132

- 一、流光简介 132
- 二、批量主机扫描 132
- 三、指定漏洞扫描 134

第3招 用ProtectX防御扫描器追踪135

- 一、ProtectX实用组件解析 135
- 二、防御扫描器攻击 136

第4招 经典嗅探器之Iris136

- 一、实例介绍Iris 136
- 二、怎样防御嗅探器 138

第5招 无线嗅探器之NetStumbler138

- 一、无线安全很重要 138
- 二、应用实战 139
- 三、拒绝笔记本Ad-hoc方式接入 140

第6招 命令行下的嗅探器WinDump140

- 一、魅力所在 140
- 二、应用实战 141

第7招 网络监听实战解析143

- 一、监听的魅力 143
- 二、监听实战 145

第8招 妙用蜜罐诱敌深入148

- 一、什么是蜜罐 148
- 二、个人级蜜罐系统的实现 149



第8章 网吧黑客的反击

第1招 网吧为何成“毒窝”151

- 一、安全问题一览 151
- 二、初识防护技术 152

第2招 网吧常见攻击与防范153

- 一、局域网攻击原理 153
- 二、局域网终结者 154

第3招 ARP欺骗实例解析155

- 一、欺骗原理 155
- 二、欺骗实例 155
- 三、ARP欺骗防范 157

第4招 网吧木马攻防158

- 一、端口映射 158

- 二、挂马实例演示 159
- 三、如何防范网吧木马 160

第5招 提升网络资源下载权限160

- 一、加密式的Flash动画下载 160
- 二、使用站点资源探测器下载 161
- 三、通过IE临时文件夹破解 162
- 四、FlashGet添加代理突破限制 162
- 五、下载在线流媒体 163

第6招 BT下载的限制与突破165

- 一、限制内网BT下载 165
- 二、突破端口封锁玩BT 167

第7招 在线解除网吧下载限制167

- 一、网吧限制的“表面文章” 167

二、利用网站在线解除限制 168

第8招 使用工具解除网吧限制 168

一、破解工具解除网吧的下载限制 168

二、使用“2008网吧破解程序” 168

三、找出作祟的网管软件 169

四、轻松搞定 网吧电影带回家 169



第9章 亦正亦邪的“远程控制”

第1招 “屏幕间谍”让你洞悉一切 171

一、屏幕间谍简介 171

二、应用实战 171

第2招 PcAnywhere远程控制 日久弥香 173

一、PcAnywhere的安装 173

二、PcAnywhere的基本设置 173

三、应用远程控制功能 174

第3招 用URLy Warning监控远程信息 175

一、软件简介 175

二、应用实战 175

第4招 用WinVNC体验远程控制 176

一、VNC简介 176

二、应用实战 176

第5招 使用QuickIP进行多点控制 177

一、QuickIP能做什么 177

二、设置服务器端 178

三、设置客户端 178

四、查看远程驱动器 179

五、远程屏幕控制 179

六、查看远程计算机进程 179

七、远程关机 179

第6招 UltraVNC轻松遥控远程电脑 179

一、被控端（服务器）设置 179

二、控制端（客户）设置 180

三、实现远程连接 180

第7招 巧用“网络人”随时远程控制 181

一、用远程IP和密码快速控制 181

二、用会员名和自定义密码连接 183

三、硬件控制器操控远程电脑 184

第8招 潜力挖掘 用好Windows远程桌面 184

一、什么是远程桌面 184

二、允许远程桌面连接 184

三、发起远程桌面连接 184

四、远程桌面和本地间传输文件 186

第9招 远程管理主机的巧妙利用 186

一、远程管理主机的利用思路 186

二、利用漏洞入侵主机 187

三、为漏洞主机打补丁 188

四、隐藏式网站建立的方法 190



第10章 网络钓鱼与网页挂马

第1招 防诈骗、防钓鱼网上安全三步走 194

一、查询对方的基本个人信息 194

二、文件安全性检查 195

三、查询网站相关信息来判断是否为骗子 195

第2招 简单百宝箱反钓鱼实战196

- 一、简单百宝箱是如何被钓鱼的 196
- 二、虚假钓鱼网站实例剖析 197
- 三、两种方法检测百宝箱是否正版 197

第3招 漏洞频曝 防范网页攻击乃当务之急 199

- 一、浏览器安全要保证 199
- 二、浏览器安全漏洞检测 199
- 三、借助杀毒软件和其他安全工具 200

第4招 逐一剖析 网页挂马实战演练200

- 一、静态网页挂马术 201
- 二、动态网页模板挂马 202
- 三、JS脚本挂马 204
- 四、Body和CSS挂马 205

第5招 Mcafee工具深入检测网站安全 206

- 一、判别网页的安全等级 206
- 二、搜索时检测网站的安全 207
- 三、查看站点详细信息 207

第6招 安全畅游网络 让“巡警”为你护驾 207

- 一、认识超级巡警账号保护神 207
- 二、屏蔽恶意网站 畅游巡警 209

第7招 用金山网盾防范网页挂马210

- 一、挂马网站快速拦截 210
- 二、对下载/传输文件安全检测 210
- 三、实时监控与一键修复 211
- 四、Flash插件轻松修复 211



第11章 黑客最青睐的“漏洞”

第1招 巧用系统更新为系统打补丁212

- 一、什么是系统漏洞 212
- 二、Windows update打补丁 212
- 三、更新并备份补丁程序 214

第2招 使用工具软件修复系统漏洞216

- 一、微软MBSA漏洞修复 216
- 二、使用360安全卫士修复漏洞 217
- 三、使用QQ修复漏洞 217

第3招 IE7“零日”漏洞攻防218

- 一、漏洞简介 218
- 二、漏洞利用代码实测 218
- 三、木马的利用 219
- 四、漏洞的防范 219

第4招 Word 0day漏洞攻防220

- 一、漏洞简介 220
- 二、攻击实战演练 220
- 三、安全防范 221

第5招 动易网站程序入侵解析222

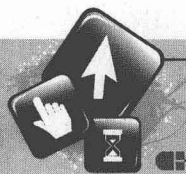
- 一、问题所在 222
- 二、入侵实战解析 223

第6招 动网程序上传漏洞入侵224

- 一、入侵实战解析 224
- 二、上传漏洞防范 226

第7招 FTP漏洞入侵实战226

- 一、FTP服务器概述 226
- 二、FTP资源大搜捕 227
- 三、对FTP服务器进行入侵 229
- 四、防范之策 230



第12章 深入浅出玩转网站攻防

第1招 轻松把握网站基本知识233

- 一、网站的结构 233
- 二、建站技术 234

第2招 网站常见攻击方式解密236

- 一、入侵管理入口 236
- 二、设计漏洞 237
- 四、网站安全十要素 240

第3招 数据库攻防实战241

- 一、初级数据库下载 241
- 二、SQL Server攻防 242
- 三、专用工具进行数据库探测 244

- 四、数据库源代码分析 245

第4招 数据库防范秘技246

- 一、本机中的数据库安全策略 246
- 二、购买空间的安全策略 246
- 三、特殊文件名法 247

第5招 严格账户管理 确保服务器安全 248

- 一、内置账户 248
- 二、账户的安全配置 250

第6招 日志管理与系统审核253

- 一、事件查看器 253
- 二、系统审核 257



第13章 反侦查的电脑安全铁律

第1招 哪些密码形同虚设260

- 一、什么样的密码才安全 260
- 二、检测密码的安全强度 260

第2招 加锁，从系统常用密码做起261

- 一、最基本：系统密码设置 261
- 二、最底层：BIOS密码设置 262
- 三、双重保护：Syskey双重加密 262
- 四、短暂离开：屏保、电源密码 263

第3招 无线网络WEP加密破解与防范 264

- 一、无线WEP加密方法 264
- 二、轻松获取WEP密码 264
- 三、当心无线WEP被破解 264
- 四、防范方法 268
- 五、消除无线安全隐患的8种手段 268

第4招 出“奇”不意 图片摇身变“加密锁” 270

- 一、新建密码箱 270
- 二、文件拖动实现快速加密 270
- 三、文件转移：密码箱拆分 271

第5招 密保卡保护 防盗号就用“巨盾” 272

- 一、全面掌控系统安全 272
- 二、三种方式查杀木马 272
- 三、首创“密保卡”方式防盗号 273
- 四、保险箱让账号更保险 273

第6招 电脑全面加锁 护卫宝一软搞定 274

- 一、文件和磁盘锁定 274
- 二、桌面和键盘锁定 275
- 三、任务管理器锁定 276
- 四、设置属于自己的密码 276

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

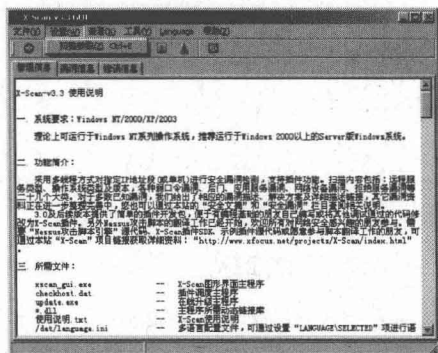
要确定目标电脑正在使用的操作系统是什么，对于初入安防之门的读者来说，推荐使用 X-Scan 来获知。

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。

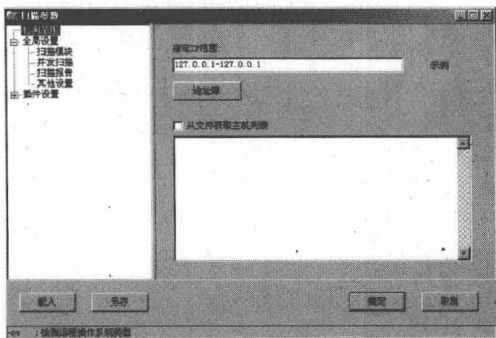
二、探测实战

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。

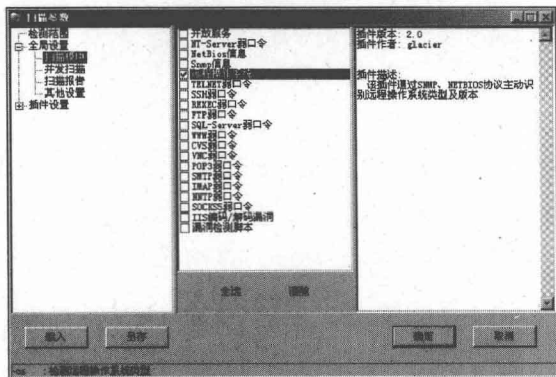
步骤 2 在完成下载并解压后，运行其中的“Xscan_gui.exe”打开如图所示的界面。



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。

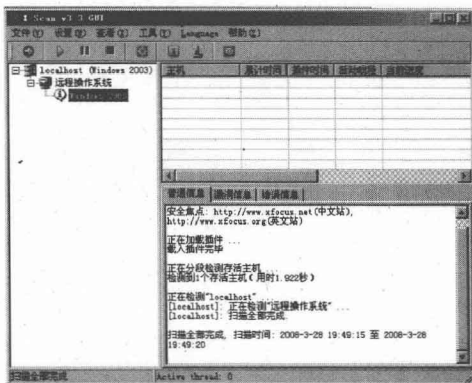


步骤4 在“全局设置”→“扫描模块”设置界面中勾选“远程操作系统”项，通过右侧的说明，可以看出远程电脑的操作系统识别是通过“SNMP、NETBIOS 协议主动识别远程操作系统类型及版本”插件来完成的，如图所示。



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”

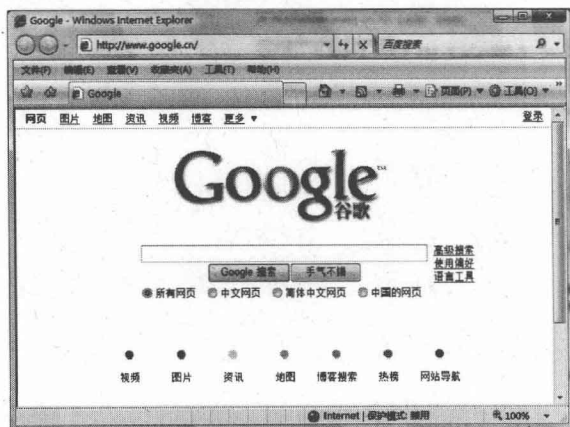
按钮后，耐心等待片刻就可以看到如图所示的扫描结果了。



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。



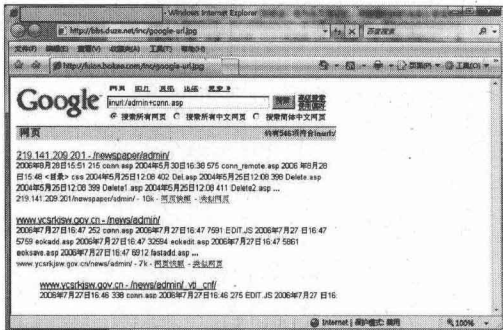
面对互联网上仅次于邮件的第二大互联网应用——搜索引擎，黑客都是怎样利用它的呢？搜索引擎对于入侵的帮助是不可或缺的，它可以帮助我们快速找到漏洞的资料、工具的下载路径、攻击的方法、存在漏洞的网站，等等。

一、搜索特殊的“关键词”

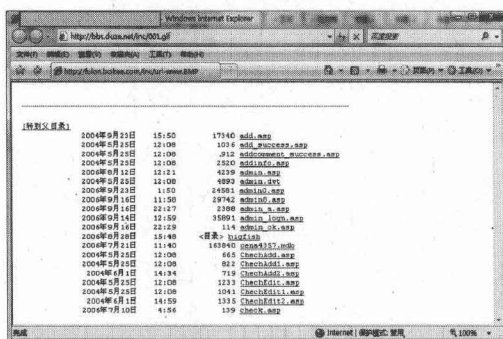
通过搜索引擎网站，黑客可以通过搜索特殊的“关键词”来查找到一些具有漏洞的网站。比方说，在动态网站中一般会有 CONN.ASP 这个文件，它用于存储数据库文件的路径、名称等信息。显然，这个文件是非常重要的，所以，黑客在搜索引擎中总是喜欢使用它作为搜索关键词，如：

inurl:/admin+conn.asp

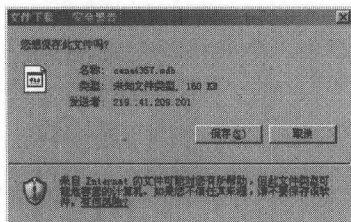
其中，admin 表示后台管理目录，它通常用于存储所有的管理文件。当然，也可以改成一些其他的目录名，但目录名要在网站中存在才行，如图所示。



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 //

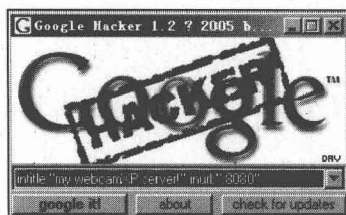
在 www.google.com 中黑客使用的关键词有很多，如 upload.asp site:tw、inurl:winnt\system32\inetsrv\ 等，这些关键词都可以为黑客起到为虎作伥的作用。

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.ysl68.com/> 下载“Google Hacker 1.2”。

接着，在“关键词”列表选择一个关键词，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.google.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。

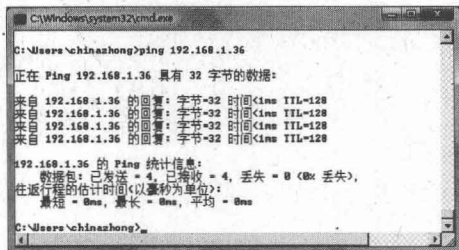
此命令的参数作用解释如下:

-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.