电脑报 总策划

一看就懂
一学就会
一本就够

绝对超值的学习套餐

图书 光盘 附赠

高品质精品图书 精品印刷、全面的功能讲解、详实的操作步骤、实用的案例演练，四大要素完美结合

多媒体视频教学 光盘收录了多媒体视频教程，播放时间长达600分钟，帮助读者互动学习，更快掌握操作技巧

新手学网络攻防

完全自学

黑客攻防入门与实战技法

黄国耀 编著

超值赠送

金山毒霸(正版杀毒软件)

让你的电脑对病毒木马永久免疫

- QQ、MSN、淘宝旺旺攻防
- 木马病毒攻防要领
- 网络账号密码防盗
- 信息与端口扫描实战
- 局域网与网吧安全策略
- 远程控制与反控制

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

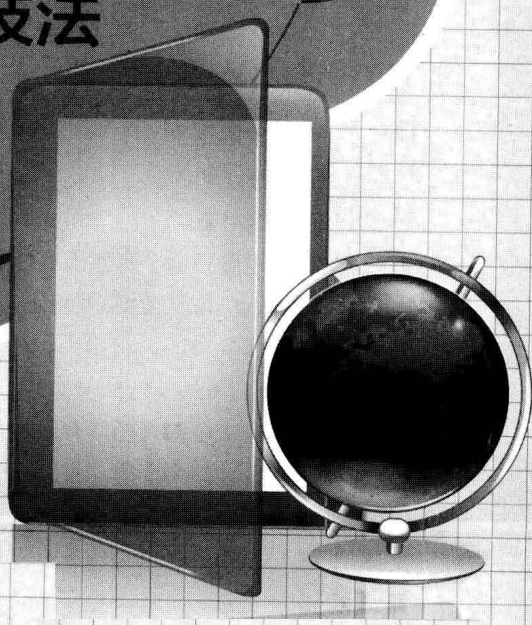
电脑报 总策划

完全自学

新手学网络攻防

黑客攻防入门与实战技法

黄国耀 编著



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

内容提要

《新手学网络攻防》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、QQ/MSN/旺旺软件攻防、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。

本书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.赠送正版杀毒软件《金山毒霸2011》

2.多媒体视频教程

- 安装虚拟机
- 清除压缩文件密码
- 清除Word密码
- 防范摄像头木马
- 黑洞木马开启摄像头
- 揪出隐藏在系统中的木马
- 利用Telnet入侵
- 开启ICP连接漏洞
- 基于ICP漏洞的入侵

3.手册配套电子书

4.黑客攻防常用工具

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。

新手学网络攻防

编　　著：黄国耀
责任编辑：李　勇
版式设计：杨　亚
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　19印张　300千字
版　　号：ISBN 978-7-89476-567-3
版　　次：2011年1月第1版　2011年1月第1次印刷
定　　价：35.00元（1CD+手册）

学电脑、用电脑的首选 Preface

《完全自学》，一本就够

- 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《完全自学》系列丛书，它是初学者的福音，更是读者电脑应用的好帮手。

作为电脑报精心筹备推出的精品大作，《完全自学》系列套书的策划、组稿和编辑工作前后历时一年。在广泛搜集了众多读者和教育专家的意见后，《完全自学》系列丛书才得以立项，之后得到了众多资深电脑教学专家的大力支持，让《完全自学》系列丛书终得以面世。

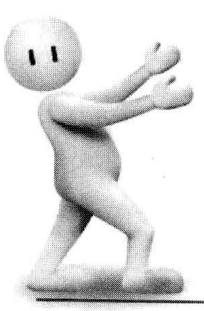
摆在读者朋友们面前的这套《完全自学》系列丛书，至少具有以下四大特色：

1．任务式教学，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需要掌握的内容，从而让读者学习没有针对性，费时费力不说，还增大了学习者的难度。

《完全自学》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！



Preface 学电脑、用电脑的首选

2．多媒体光盘教学，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，总会遇到这样那样的问题，这其实就是实战经验不足或动手操作太少的缘故。《完全自学》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．信息量大，每本都可以独立当作一部“大全”手册使用

《完全自学》系列使用“任务式”教学模式。《完全自学》系列的每一本图书都是这一类别中的“小权威”，体现了“大全”的思路，学此一本就可以从头开始完全掌握某一领域的操作与应用。

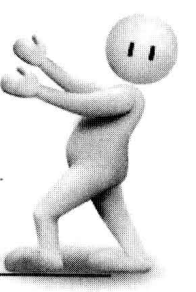
4．随光盘附赠超值杀毒软件，让电脑安全无忧

光盘中还特别赠送了正版的金山毒霸2011，可将藏身于系统中的病毒、木马、恶意软件等威胁一网打尽，有力保障电脑用户的安全。软件还具有超强自我保护功能，能免疫所有病毒杀软功能失效的非法控制。

《完全自学》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，直接学习更为综合的进阶应用。

最后，祝愿所有的读者都能在《完全自学》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



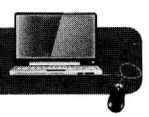
试读结束：需要全本请在线购买：　www.ertongbook.com

新手学网络攻防 目录
CONTENTS

第1讲 黑客入侵前的信息搜集

第1课 操作系统和网站信息搜集 …… 2
1.1 搜集操作系统版本 …… 2
1.X-Scan介绍 …… 2
2.探测步骤 …… 2
3.通过网站判断 …… 3
1.2 Google也能探测有漏洞的网站 …… 3
1.搜索特殊的“关键词” …… 4
2.Google Hacker威力无穷 …… 4
1.3 网站经常导致信息泄密 …… 5
1.域名基础知识 …… 5
2.探测域名与IP …… 6
3.用Nslookup命令查询IP相关信息 …… 7
4.获得网站基本信息资料 …… 8
5.查看网站备案登记信息 …… 9
6.查看网站其他信息 …… 10
第2课 几种基本的信息搜集与筛选方法 10
2.1 认识黑客社会工程学攻防 …… 10
1.什么是社会工程学 …… 10
2.黑客社会工程学的常用手段 …… 11
2.2 QQ、博客中的信息搜集 …… 12
1.挖掘你需要的QQ号 …… 12
2.通过博客挖掘更多信息 …… 13
3.从QQ开始“探路” …… 14
4.不容忽视的QQ群 …… 14
2.3 信息筛选有诀窍 …… 15
1.人工筛选信息 …… 15
2.软件筛选信息 …… 17
3.社会工程学 …… 18
第3课 隐藏IP信息增强安全 …… 19
3.1 为什么要隐藏IP …… 19
3.2 使用代理藏IP …… 20
3.3 使用提供匿名冲浪的网站隐藏IP 20
3.4 Telnet入侵时隐藏IP …… 21
3.5 使用工具软件藏IP …… 21
3.6 验证IP是否隐藏成功 …… 22
小知识：网络炸弹 …… 22
第4课 保护个人信息拒绝做“肉鸡” … 23
4.1 什么是“肉鸡” …… 23
4.2 如何判断电脑是否成为“肉鸡” 24
1.QQ、MSN、网游等有异常登录提醒 24
2.键盘、鼠标、摄像头不听使唤 … 24
3.硬盘灯、网卡灯狂闪 …… 24
4.3 使用工具软件检测是否为“肉鸡” 25
1.使用Tcpview检测网络连接 …… 25
2.使用“金山肉鸡检测器” …… 25

第2讲 QQ、MSN盗号与防范实例



第1课 QQ常见的盗号和骗局 …… 28
1.1 为何收文件后QQ就被盗 …… 28
1.盗号骗局再现 …… 28
2.双格式文件实例解析 …… 28

3.防盗技巧 …… 29
1.2 识破“QQ靓号”的骗局 …… 29
1.“QQ靓号”的诱惑 …… 29
2.安全防范技巧 …… 30
第2课 QQ密码攻防实例 …… 31
2.1 防范QQ终结者在线盗号 …… 31
1.配置盗号木马 …… 31
2.上传文件、收获密码 …… 32
2.2 黑客用偷窥者盗取QQ …… 32
1.配置“偷窥者” …… 33
2.把本机的IP更新到空间 …… 33
3.发送服务端给被攻击者 …… 34
4.捕获肉鸡 …… 34
2.3 “QQ远控精灵”远程控制计算机 34
1.QQ远控精灵介绍 …… 34
2.远程控制实例 …… 35
3.防范措施 …… 36
2.4 防范“啊拉QQ大盗”盗取QQ … 36
1.邮箱收信 …… 37
2.网站收信 …… 38
3.“啊拉QQ大盗”防范方法 …… 38
2.5 防范“QQ大杀器”盗QQ …… 39
1.QQ号、Q币、密保都遭殃 …… 39
2.自动生成QQ尾巴 …… 40
3.文件捆绑、自动弹出网页 …… 40
小知识：什么是服务 …… 41
第3课 QQ安全防范实战 …… 41
3.1 QQ存在哪些安全隐患 …… 41
3.2 获取QQ空间最高权限 …… 42
3.3 QQ聊天记录安全防范 …… 44
3.4 强行聊天防范 …… 45
3.5 QQ炸弹防范 …… 46
3.6 IP地址攻防 …… 48
3.7 恶意链接防范 …… 49
小知识：如何识别骗子网站 …… 52
第4课 Windows Live Messenger安全防范 52
4.1 MSN聊天记录防范 …… 53
4.2 MSN强行聊天防范 …… 56
第5课 当心！淘宝旺旺密码也被“盗” 57
5.1 旺旺进程中“明文”保存密码账号57
5.2 旺旺中登录邮箱也“明文”显示 58

第3讲 加密、解密与突破实例剖析

第1课 文件另类隐藏与加密 …… 60
1.1 隐藏：让文件夹彻底“消失” … 60
1.更改文件夹图标 …… 60
2.隐藏文件名 …… 61
3.更改特殊文件名 …… 61
4.巧用“文件更名”让文件“蒸发” ……61
1.2 “自动销毁”式文件加密 …… 63
1.巧借网站实现自动销毁 …… 63
2.软件让你保护机密文件 …… 64
3.文件自动销毁也有“回天术” … 65
1.3 杀毒软件也能“隐藏”机密文件 67
1.杀毒软件的副业：文件隐藏 …… 67
2.机密文件提取 …… 68
3.机密文件不泄密 …… 68
第2课 常见密码加密与破解解析 …… 69
2.1 当心系统密码被破解 …… 69
1.Syskey双重加密 …… 69
2.轻松创建“开机软盘” …… 70
2.2 巧妙解除NOD32的密码保护 …… 70
1.NOD32个人密码设定 …… 71
2.修改注册表清除密码 …… 71
3.使用专用工具“解锁” …… 71
2.3 暴力破解路由器揭秘 …… 72
1.破解无线路由器账号、密码 …… 72
2.修改无线网络密码 …… 73
小知识：明文和密文 …… 74
2.4 用RAR Password Cracker恢复RAR密码 74
1.创建加密文件 …… 74

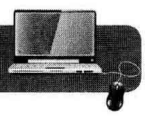
2.恢复RAR文件密码 …… 74
2.5 破解压缩文件密码 …… 75
1.WINZIP压缩文件的破解 …… 76
2.WINRAR压缩文件的破解 …… 76
3.巧妙设置，让压缩文件无懈可击 77
第3课 使用加密工具保护隐私 …… 78
3.1 虚拟磁盘加密隐藏隐私 …… 78
1.创建虚拟加密磁盘 …… 78
2.虚拟磁盘的使用 …… 79
3.2 文件隐藏大师 …… 81
1.创建隐藏文件夹 …… 81
2.操纵“隐藏文件夹” …… 81
3.编辑和删除隐藏文件夹 …… 82
4.文件隐藏大师项设置 …… 82
3.3 查看谁动了我的文件 …… 83
1.防止别人进行新建、复制操作 … 83
2.禁止改名、移动文件 …… 84
3.禁止删除文件 …… 84
4.设置解锁密码 …… 84
5.查看监控记录 …… 85
6.保护特定的文件夹 …… 85
3.4 军用级硬盘加密 …… 85
1.创建虚拟磁盘空间 …… 86
2.对数据文件加密 …… 87
3.在虚拟磁盘中创建“虚拟磁盘” 87

第4讲 局域网与网吧安全攻防

第1课 局域网环境下的安全隐患 …… 90
1.1 隐患一：局域网成病毒“窝” … 90
1.2 隐患二：局域网盗号 …… 90
1.3 隐患三：网络被攻击 …… 91
1.4 隐患四：局域网共享文件安全 … 91
第2课 Windows XP中如何实现安全共享 91
2.1 禁用简单文件共享 …… 91
2.2 创建用户账户和用户组 …… 92
2.3 共享文件 …… 92
2.4 设置共享权限 …… 92
2.5 巧用组策略增强Windows XP共享安全 93
1.修改组策略指定特定用户访问 … 93
2.禁止非法用户访问 …… 93
第3课 简单几招封杀系统默认共享 …… 94
3.1 “停止共享”法 …… 94
3.2 批处理自启动法 …… 95
3.3 修改注册表法 …… 95
3.4 停止服务法 …… 96
3.5 卸载“文件和打印机共享”法 … 96
小知识：域和工作组 …… 97
第4课 Vista下如何实现安全共享 …… 97
4.1 Vista文件共享方法 …… 97
4.2 设置访问权限增强安全 …… 99
第5课 共享漏洞攻防实例演示 …… 99
5.1 使用工具扫描 …… 99
5.2 配合IPC$ ……100
5.3 窃取共享密码 ……103
第6课 共享漏洞安全防范 ……104
6.1 安全策略配置 ……104
1.策略一：空密码登录 …… 104
2.策略二：网络拒绝登录 …… 105
6.2 权限设置与管理 ……106
1.认识共享权限 …… 106
2.基本共享权限 …… 107
3.高级共享权限 …… 108
4.防火墙与共享权限 …… 109
5.共享权限与NTFS权限 …… 111
第7课 局域网攻击实例剖析 …… 111
7.1 局域网攻击原理 ……111
7.2 局域网终结者实例剖析 ……112
第8课 ARP欺骗攻防实例 …… 113
8.1 ARP欺骗原理 ……113
8.2 ARP欺骗实例解析 ……114

8.3 ARP欺骗防范 ……116
1.方法一：绑定IP和MAC地址 …… 116
2.方法二：编写批处理文件 …… 116
3.方法三：使用“金山ARP防火墙”工具 …117
动手练一练：查看IP地址与MAC地址 118

第5讲 木马、病毒攻击与防范



第1课 常见木马入侵手法 …… 120
1.1 木马入侵途径分析 ……120
1.2 木马的运行原理 ……120
1.木马的工作方式 …… 120
2.木马的隐身启动术 …… 120
3.木马如何将入侵主机信息发送给攻击者 …121
1.3 木马隐形位置 ……122
1.集成到程序中 …… 122
2.隐藏在配置文件中 …… 122
3.潜伏在Win.ini中 …… 122
4.伪装在普通文件中 …… 122
5.内置到注册表中 …… 122
6.在System.ini中藏身 …… 123
7.隐形于启动组中 …… 123
8.隐蔽在Winstart.bat中 …… 123
9.捆绑在启动文件中 …… 123
10.设置在超级连接中 …… 123
第2课 最经典的木马——冰河 …… 124
2.1冰河入侵与反入侵实战 ……124
1.木马入侵 …… 124
2.木马反入侵 …… 126
2.2 反弹式木马的反入侵 ……127
1.什么是反弹式木马 …… 127
2.监控反弹木马的端口 …… 127
第3课 RM影片木马攻防实战 …… 128
3.1 影片木马的特点 ……128
3.2 RM影片木马制作 ……129
1.让影片在播放时自动弹出浏览器窗口 … 129
2.在网页中添加木马 …… 131
3.3 RM影片木马的防范 ……131
第4课 听歌也会中木马 …… 132
4.1 MP3中挂木马的原理 ……132
4.2 添加音乐文件 ……132
4.3 设置弹窗方式和弹出时间 ……133
4.4 设置木马网页地址 ……133
4.5 MP3音乐“木马”防范措施 ……134
第5课 图片中“捆绑”木马 …… 135
5.1 图片与程序的“捆绑” ……135
5.2 用COPY命令来捆绑 ……136
5.3 使用专用工具“捆绑” ……136
1.“捆绑”加密 …… 136
2.解密 …… 137
第6课 木马加壳与脱壳 …… 138
6.1 木马加壳的方法 ……138
1.什么是加壳 …… 138
2.加壳实战 …… 138
6.2 检测加壳方式 ……140
6.3 木马脱壳实战 ……140
第7课 认识计算机病毒 …… 142
7.1 什么是病毒、蠕虫、木马 ……142
1.什么是病毒 …… 142
2.什么是蠕虫 …… 142
3.什么是特洛伊木马 …… 142
7.2 计算机病毒的传染途径 ……142
1.软盘 …… 143
2.光盘 …… 143
3.硬盘 …… 143
4.优盘 …… 143
5.网络 …… 143
7.3 病毒发作实例演示 ……144
7.4 遭遇病毒时的应急措施 ……145
1.清空IE临时文件 …… 145
2.显示所有文件和文件夹 …… 146

3.进入安全模式 …… 146
4.查看并禁用服务 …… 146
第8课 在虚拟机中实测病毒木马 …… 147
8.1 认识虚拟机 …… 147
8.2 虚拟机安装实战 …… 148
8.3 打造自己的虚拟计算机 …… 148
8.4 文件共享 …… 152
8.5 虚拟机中的病毒木马实战 …… 153
第9课 使用工具清除病毒、木马 …… 155
9.1 使用金山毒霸查杀病毒与木马 …… 155
1.软件安装与升级 …… 155
2.快速杀毒 …… 155
3.实时监控 …… 156
4.系统清理 …… 157
9.2 微点主动防御软件杀木马 …… 157
1.安全防护 …… 157
2.漏洞扫描 …… 158
3.设置自动防护 …… 158
4.控制进程保安全 …… 158
5.查杀未知木马 …… 159
6.日志管理 …… 159
小知识：什么是日志 …… 160
1.日志的特殊性 …… 160
2.黑客为什么会对日志文件感兴趣 160
动手练一练：命令行轻松防病毒 …… 161
1.Tasklist揪出可疑进程 …… 161
2.Ntsd结束病毒进程 …… 161
3.Find查看文件是否被捆绑 …… 162
4.FC检查注册表是否被篡改 …… 162

第6讲 进程与端口攻防实例

第1课 认识Windows进程 …… 164
1.1 关闭进程和重建进程 …… 164
1.关闭进程 …… 164
2.新建进程 …… 164
1.2 查看进程的发起程序 …… 165
第2课 关闭恶意进程 …… 166
2.1 关闭任务管理器杀不了的进程 …… 166
1.哪些系统进程不能关掉 …… 166
2.关闭任务管理器杀不了的进程 … 166
2.2 查看隐藏进程和远程进程 …… 167
1.查看隐藏进程 …… 167
2.查看远程进程 …… 167
2.3 杀死病毒进程 …… 168
第3课 进程攻防实例解析 …… 168
3.1 当心病毒寄生SVCHOST.EXE进程 168
1.认识SVCHOST.EXE …… 168
2.识别SVCHOST.EXE进程中的病毒 … 169
3.2 判断Explorer.exe进程真假 …… 170
1.什么是Explorer.exe进程 …… 170
2.Explorer.exe容易被冒充 …… 170
3.3 巧用Windows进程管理器 …… 172
1.进程管理 …… 172
2.恶意进程分析 …… 172
3.4 超级巡警保护系统进程 …… 172
1.全面查杀 …… 173
2.实时防护 …… 173
3.保险箱 …… 173
4.系统安全增强工具 …… 174
5.妙用SSDT工具清除流氓软件 …… 175
第4课 认识系统端口 …… 175
4.1 端口的分类 …… 175
1.已知端口 …… 176
2.注册端口 …… 176
3.动态端口 …… 176
4.2 开启和关闭端口 …… 176
1.查看端口 …… 176
小知识：Netstat命令用法 …… 177
2.关闭端口 …… 177
3.开启端口 …… 177
4.3 端口查看工具 …… 177
4.4 重定向本机默认端口 …… 178

1.在本机上(服务器端)修改 …… 178
2.在客户端上修改 …… 179
第5课 端口攻防与扫描实例 …… 179
5.1 3389端口入侵与防范 …… 179
1.什么是3389端口 …… 179
小知识：什么是“肉鸡”？ …… 180
2. 3389入侵实例剖析 …… 180
3. 3389端口安全防范 …… 181
5.2 扫描端口确保电脑安全 …… 181
1.常见端口剖析 …… 181
2. 用SuperScan扫描端口安全 …… 182
动手练一练：用NetBrute Scanner扫描端口183

第7讲 常见漏洞攻防实例

第1课 认识系统漏洞攻防 …… 186
1.1 系统漏洞的基本概念 …… 186
1.2 系统漏洞的自动修补 …… 186
1.使用Windows XP自带的系统“自动更新”功能 …… 187
2.使用BigFix修复 …… 187
1.3 轻松备份补丁文件 …… 189
第2课 系统漏洞检测与修复 …… 190
2.1 微软MBSA检测漏洞 …… 190
1.漏洞检测 …… 190
2.查看检测报告 …… 191
2.2 检测内网计算机的安全漏洞 …… 191
1.认识安全扫描专家 …… 191
2.扫描实战 …… 192
第3课 IE7 0day漏洞攻防实例 …… 195
3.1 漏洞简介 …… 195
3.2 漏洞利用代码实测 …… 195
3.3 木马利用实例 …… 196
3.4 漏洞的防范 …… 197
第4课 网站、论坛的噩梦：PHPWind漏洞197
4.1 PHPWind漏洞入侵实例剖析 …… 197
4.2 PHPWind漏洞防范 …… 199
1.安装漏洞补丁 …… 199
2.修改论坛创始人密码 …… 199
3.密码修复 …… 199
4.使用安全检测工具 …… 199
第5课 Windows logon溢出工具体验 …… 200
5.1 认识缓冲区溢出漏洞 …… 200
5.2 远程溢出实战 …… 200
5.3 漏洞防范 …… 201
第6课 DcomRpc漏洞溢出入侵与防范 … 201
6.1 什么是Dcom和Rpc …… 201
6.2 什么是溢出入侵 …… 202
6.3 DcomRpc漏洞入侵解析 …… 203
6.4 DcomRpc漏洞安全防范 …… 204
1.打好补丁 …… 204
2.封锁135端口 …… 204
3.关闭RPC服务 …… 205
4.手动为计算机启用(或禁用)DCOM … 205
动手练一练：Flash漏洞攻防 …… 206
1.漏洞利用解析 …… 206
2.漏洞分析与防范 …… 207

第8讲 黑客远程监控实例剖析

第1课 巧用“网络人”远程控制随时随地 210
1.1 无需注册 用远程IP和密码快速控制 210
1.远程控制基本设置 …… 210
2.远程控制设置 …… 211
3.文字聊天与文件传输 …… 211

试读结束：需要全本请在线购买：www.ertongbook.com

4.让对方控制我 …… 212
1.2 永不更改 用会员名和自定义密码连接212
第2课 远程桌面入侵与防范 …… 213
2.1 入侵实战解析 …… 213
2.2 安全防范 …… 216
1.对端口进行安全管理 …… 216
2.快速判断入侵迹象并采取果断措施 … 217
第3课 用灰鸽子进行远程监控 …… 219
3.1 灰鸽子简介 …… 219
3.2 生成服务器端 …… 219
3.3 查看控制效果 …… 220
3.4 禁止灰鸽子服务 …… 220
3.5 彻底清除 …… 221
3.6 解除关联 …… 221
第4课 用WinVNC实现远程控制 …… 222
4.1 WinVNC简介 …… 222
4.2 WinVNC监控应用实战 …… 222
1.配置服务器 …… 222
2.客户端连接 …… 223
3.WinVNC的高级应用 …… 223
第5课 QuickIP进行多点远程控制 …… 224
5.1 QuickIP能做什么 …… 224
5.2 设置服务器端 …… 225
5.3 设置客户端 …… 226
5.4 查看远程驱动器 …… 226
5.5 远程屏幕控制 …… 226
5.6 查看远程计算机进程 …… 227
5.7 远程关机 …… 227
第6课 UltraVNC实现监控远程电脑 …… 227
6.1 被控端设置 …… 227
6.2 控制端设置 …… 228
6.3 实现远程连接 …… 228
第7课 屏幕间谍定时抓屏监控 …… 229
7.1 屏幕间谍简介 …… 229
7.2 应用实战 …… 230
动手练一练：动手制作远程控制程序 231
1.合并EXE文件 …… 231
2.修改合并后的EXE文件图标 …… 232

第9讲 网络钓鱼与网页挂马

第1课 网络钓鱼攻防实例 …… 234
1.1 简单百宝箱反钓鱼实战 …… 234
1.简单百宝箱是如何被“钓鱼”的 234
2.虚假钓鱼网站实例剖析 …… 234
3.两种方法检测百宝箱是否正版 … 235
1.2 网络钓鱼防范三步走 …… 236
1.第一步：查询对方的基本个人信息 … 236
2.第二步：文件安全性检查 …… 237
3.第三步：查询网站相关信息来判断是否为骗子 … 238
第2课 网页挂马实战解析 …… 239
2.1 漏洞频曝 防范网页攻击乃当务之急239
1.浏览器安全要保证 …… 239
2.浏览器安全漏洞检测 …… 240
3.借助杀毒软件和其他安全工具 … 241
2.2 网页挂马实战演练 …… 242
1.静态网页挂马术 …… 242
2.动态网页模板挂马 …… 243
3.JS脚本挂马 …… 246
4.Body和CSS挂马 …… 246
第3课 多管齐下防范网页挂马 …… 248
3.1 McAfee工具深入检测网站安全 …248
1.判别网页的安全等级 …… 248
2.搜索时检测网站的安全 …… 249
3.查看站点详细信息 …… 249
3.2 超级“巡警”让你畅游网络 ……250
1.加个保险箱 超级巡警账号保护神…… 250
2.屏蔽恶意网站 畅游巡警 …… 251
3.3 用金山网盾防范网页挂马 ……252

1.挂马网站快速拦截 …… 252
2.对下载/传输文件进行安全检测 … 253
3.实时监控与一键修复 …… 254
4.Flash插件轻松修复 …… 254

第10讲 网站与服务器攻防实例

第1课 网站攻防基础知识 …… 256
1.1 网站架构 …… 256
1.2 网站建站技术解析 …… 257
1.静态网页技术 …… 257
2.动态网页技术 …… 257
3.源代码 …… 258
4.路径 …… 259
第2课 网站常见攻击方式揭秘 …… 260
2.1 入侵网站管理入口 …… 260
2.2 网页木马入侵 …… 261
2.3 网站漏洞攻击 …… 263
2.4 网站安全维护要点 …… 266
第3课 网站数据库攻防 …… 267
3.1 最简单的数据库下载 …… 268
3.2 SQL Server攻防 …… 269
3.3 使用专用工具探测数据库 …… 271
3.4 网站源代码分析 …… 272
3.5 数据库安全防范要领 …… 273
1.本机中的数据库安全策略 …… 273
2.购买空间的安全策略 …… 274
3.特殊文件名法 …… 275
第4课 服务器攻防解析 …… 276
4.1 服务器安全基础知识 …… 276
4.2 通过服务器漏洞入侵 …… 277
4.3 服务器软件的安全“隐患” …… 278
1.设置不当 …… 279
2.Serv-U漏洞实战 …… 280
4.4服务器账户安全管理 …… 281
1.内置账户 …… 282
2.账户的安全配置 …… 284
第5课 日志安全管理 …… 288
5.1 认识事件查看器 …… 288
5.2 事件日志的类型 …… 289
5.3 查看事件 …… 291

Chapter 01

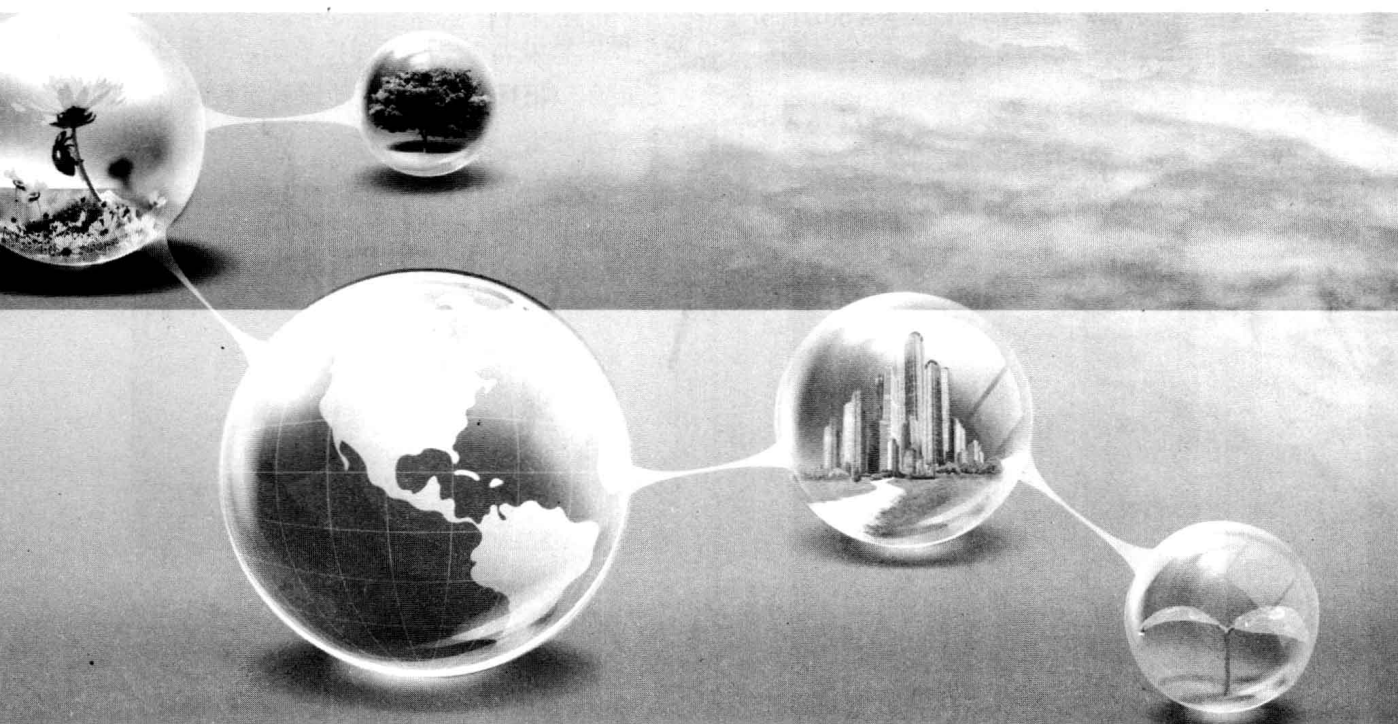
多媒体教学视频光盘

第1讲 黑客入侵前的信息搜集

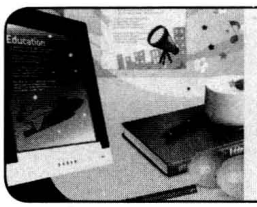
当网络逐步普及，“黑客”这个词就逐步走入我们的生活，黑客并不遥远，你需要随时做好防范方能在复杂的网络环境中不被他人攻击！那么，黑客入侵前到底需要了解哪些信息才能发动攻击呢？在本讲中将首先为大家剖析黑客攻防中的信息搜集工作，这主要包括被攻击机器的操作系统、漏洞、端口开放情况等，而网络、QQ、博客等地方将很有可能成为黑客搜集信息的场所。

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。

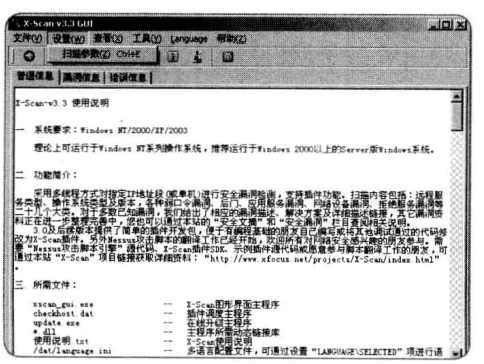
1.X-Scan介绍

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

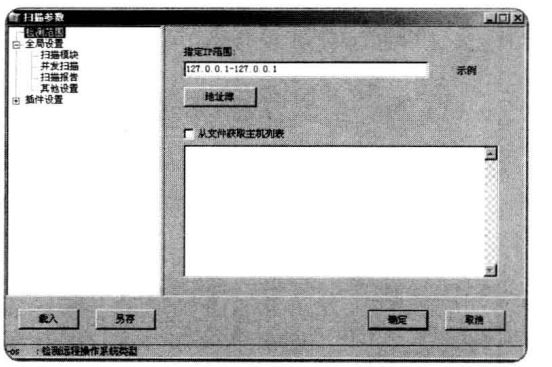
步骤01 首先，到国内著名的安全网站“安全焦点”（“http://www.xfocus.net/tools/200507/1057.html”）下载X-Scan v3.3 中文版。

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。



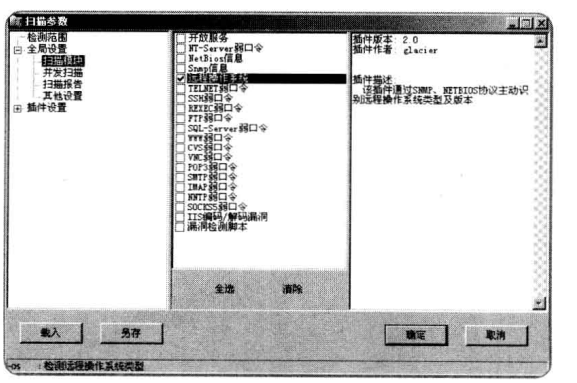
▲ Xscan软件

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：

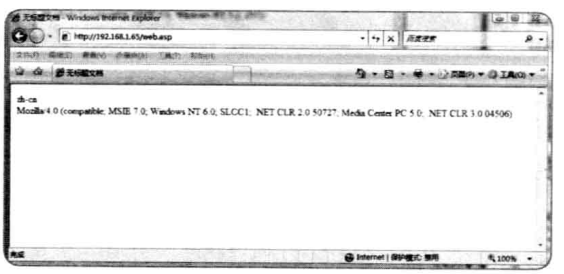
某黑客与某个人电脑用户通过QQ聊天，黑客说：“我的网站不错，欢迎你来访问。”，并给出一个网页地址。很多个人电脑用户不会提防这个要求，于是立即访问了这个网页。

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也能探测有漏洞的网站

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

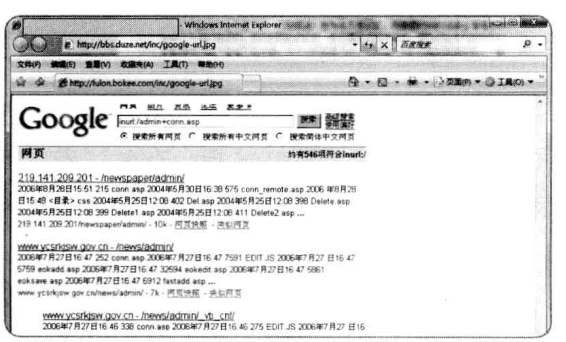
面对互联网上仅次于邮件的第二大互联网应用——搜索引擎，黑客都是怎样利用它的呢？搜索引擎对于入侵的帮助是不可或缺的，它可以帮助我们快速找到漏洞的资料、工具的下载路径、攻击的方法、存在漏洞的网站，等等。

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：

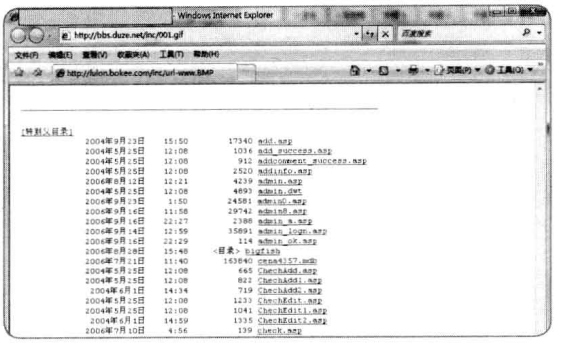
inurl:/admin+conn.asp

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。



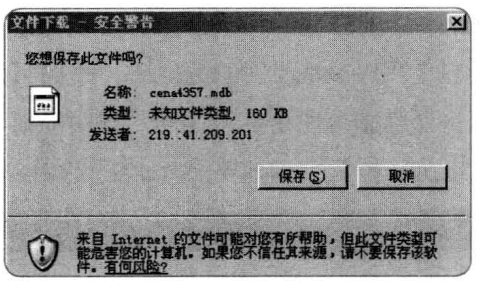
▲ 搜索关键词

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

试读结束：需要全本请在线购买： www.ertongbook.com