

黑客攻防

最佳十一人

网络攻击、防御实例演练



前锋：进攻！一击致命

系统漏洞与网站漏洞攻击
暴力攻击与恶意绑架



后卫：防卫！转危为安

网络盗号与防范
病毒查杀与防范
网络提权与网吧攻防
数据的加密与解密

黄国耀 李国良 编著



中场：创意！制造杀机

远程控制与反控制
信息收集与行踪隐藏
网络嗅探与监控
木马植入与防范



守门：不可逾越的防线

网络安全终极防范

111招攻守博弈！

彻底破解黑客攻防之道！！
成就安全大师！！



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

黑客攻防

最佳十一人

网络攻击、防御实战演练

藏书章

黄国耀 李国良 编著

内容提要

本手册专为黑客技术与网络安全爱好者量身定制，以实例演练形式为读者详细剖析黑客攻防手段，并提供相应防护措施。手册内容共计 11 章，内容涵盖信息收集与行踪隐藏、网络嗅探与监听、木马植入与防范、远程控制与反控制、系统漏洞与网站漏洞攻击、暴力攻击与恶意绑架、网络盗号与防范、病毒查杀与防范、网络提权与网吧攻防、数据的加密与解密、网络安全终极防范。丰富的案例、详尽的操作步骤将给读者提供最快捷的帮助，迅速掌握黑客与网络安全技术。

警告：本手册及光盘涉及到的黑客相关知识，仅供读者研究、学习参考，请勿用于非法用途，否则后果自负。

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

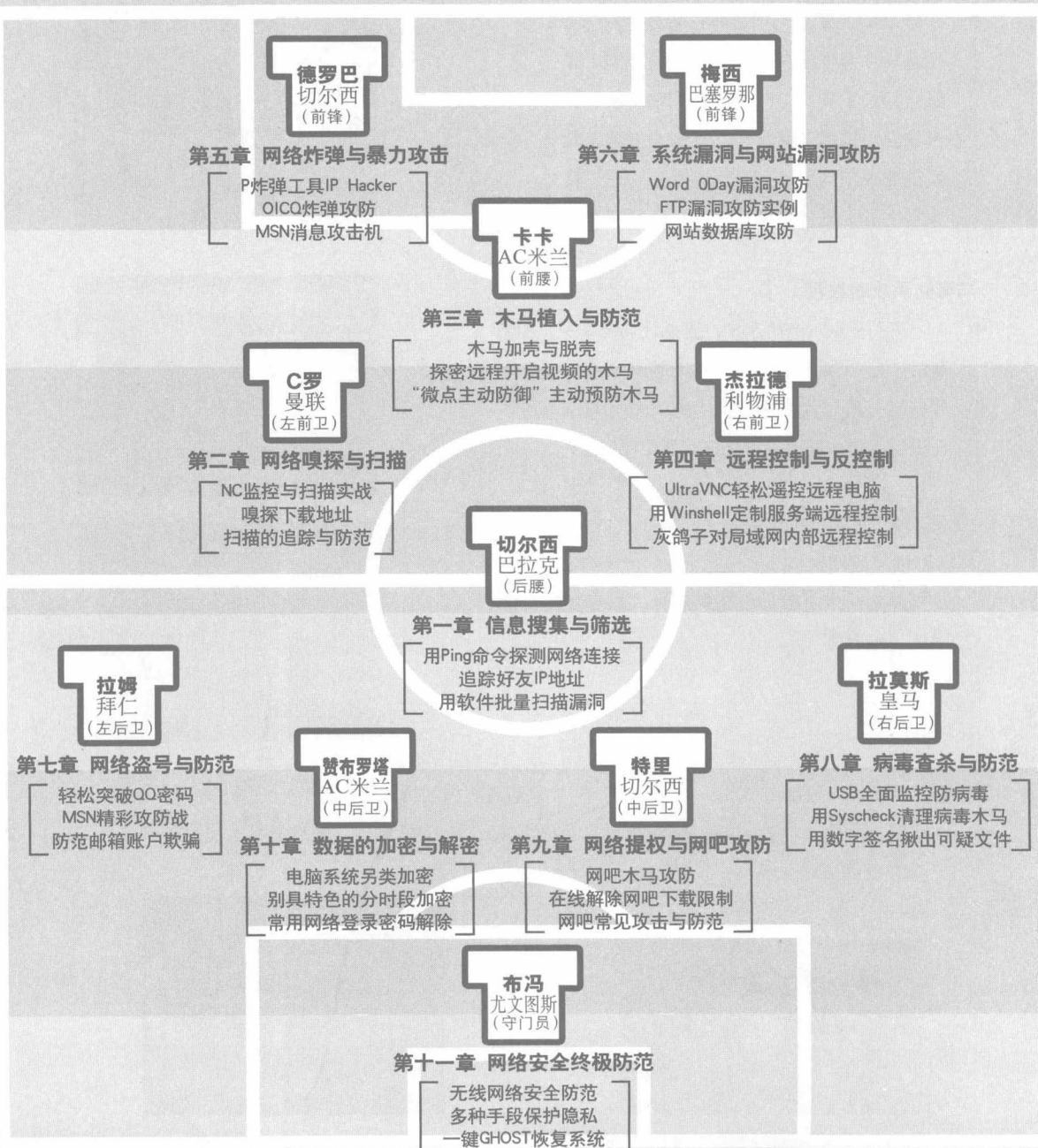
手 册 名：黑客攻防最佳十一人
编 著：黄国耀 李国良
技术编辑：连 果 李 勇
封面设计：朱 姝
出版单位：电脑报电子音像出版社
地 址：重庆市双钢路3号科协大厦
邮 政 编 码：400013
对外合作：(023)63658933
发 行：电脑报经营有限责任公司
经 销：各地新华书店、报刊亭
C D 生 产：苏州新海博数码科技有限公司
文 本 印 刷：重庆科情印务有限公司
开 本 规 格：787mm × 1092mm 1/16 19印张 350千字
版 号：ISBN 978-7-89476-128-6
版 次：2009年4月第1版 2009年4月第1次印刷
定 价：32.00元(1CD+1手册)

攻守兼备

黑客攻防最佳“十一人”

进攻，无坚不摧；防守，固若金汤。电光火石之间，他们亦能转危为安。这是一支攻守兼备、令人生畏的球队。十一人，或攻或防，进退自如，将足球运动的精髓演绎得如此完美。那么，你想拥有这样一支战无不胜的球队吗？你想拥有这样攻守兼备的“十一人”吗？

不可能？谁说不可能！在我们的电脑、网络生活中，我们同样可以雇佣这样的十一位“铁血硬汉”，打造一支攻守兼备的完美战队。攻，可如探囊取物般行走于网络；防，可坚如磐石般抵御他人不轨侵袭。不同的十一人，同样的攻守兼备，你不想一试身手吗？现在，这“十一人”将一一亮剑，展示他们的能力和技巧，用好了他们，你将彻底玩转黑客攻防，成就安全大师。



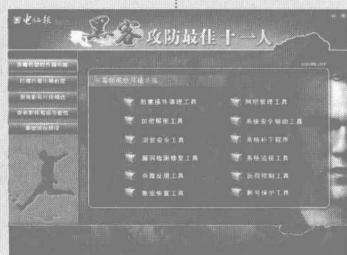
光盘导航

全面、实用 黑客攻防工具大全
光盘可自启动、可自动杀毒防黑



杀毒防黑软件精华库

- 杀毒反黑工具
- 恶意插件清理工具
- 账号保护工具
- 系统安全辅助工具
- 系统监视工具
- 数据恢复工具
- 漏洞检测修复工具
- 远程控制工具
- 加密解密工具
- 浏览安全工具
- 网吧管理工具
- 系统补丁程序



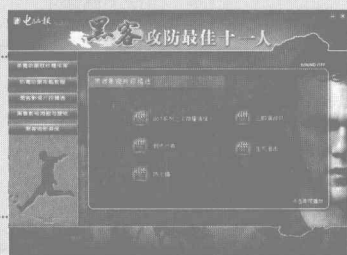
防毒防黑攻略教程

- 高手指点，亲历亲学，查杀现场全掌握。2008灰鸽子超级简单免杀、个人电脑安全设置、揭示局域网抓鸡过程演示、揭示另类木马躲避杀毒软件过程、清除被感染系统中的病毒代码。



黑客影视片段精选

- 经典谍战电影片段精彩欣赏，感受真实、震撼的现场氛围。



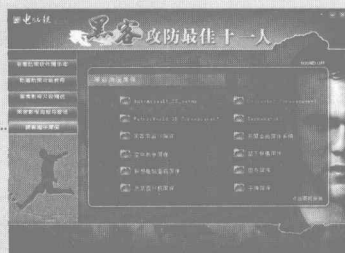
黑客影视海报与壁纸

- 超20幅谍战电影海报、壁纸欣赏，让精彩瞬间留住永恒。



黑客绚丽屏保

- 保护屏幕，酷炫桌面，质感体验。





CONTENTS

目录



中场：创意！制造杀机



第一章 巴拉克——信息搜集与筛选



第一招 巧用 X-scan 探测系统版本·····2

- 一、设置扫描参数 ·····2
- 二、开始扫描 ·····3
- 三、查看操作系统版本 ·····3

第二招 用 Ping 命令探测网络连接·····3

- 一、Ping命令参数介绍 ·····3
- 二、Ping命令探测实例 ·····4

第三招 通过网站获取操作系统信息 ·····5

- 一、获取系统信息的代码 ·····5
- 二、查看系统版本信息 ·····5

第四招 追踪好友 IP 地址·····6

- 一、网络定位 ·····6
- 二、获取好友IP地址 ·····7
- 三、追踪更多信息 ·····7

第五招 探测网站域名和 IP 信息·····9

- 一、域名基础知识 ·····9
- 二、探测域名与IP ·····10

三、用Nslookup命令查询IP相关信息 ·····10

第六招 获取网站的注册信息·····12

- 一、获得网站基本信息资料 ·····12
- 二、查看网站备案登记信息 ·····13
- 三、查看网站其他信息 ·····13

第七招 用搜索引擎探测网站漏洞·····13

- 一、探测网站的漏洞 ·····14
- 二、Google Hacker探测实例 ·····15

第八招 用软件批量扫描漏洞·····15

- 一、扫描准备 ·····15
- 二、选择扫描引擎 ·····17
- 三、FTP漏洞扫描 ·····18

第九招 信息分析与筛选·····19

- 一、人工筛选 ·····19
- 二、软件筛选 ·····20
- 三、社会工程学筛选 ·····21



第二章 C 罗——网络嗅探与扫描



第一招 嗅探 FTP 口令实例 ·····24

- 一、什么是嗅探程序 ·····24
- 二、嗅探窃密的原理 ·····24
- 三、嗅探FTP口令实例 ·····24
- 四、如何防范嗅探 ·····25

第二招 Iris 嗅探数据实例 ·····26

- 一、Iris的工作原理 ·····26
- 二、用Iris捕获数据 ·····27
- 三、Iris嗅探的防御方法·····29

第三招 用 WinDump 在命令行嗅探·····29

- 一、软件特色 ·····29
- 二、应用实战 ·····30

第四招 “影音嗅探专家”嗅探影片下载地址	31	第七招 RPC 漏洞扫描器	41
一、安装配置	31	一、RPC漏洞带来的危险	41
二、下载设置	32	二、RPC 漏洞介绍	41
三、嗅探实战	32	三、扫描RPC漏洞	42
四、其他功能	33	第八招 Webdavscan 漏洞扫描器	42
第五招 Sss 扫描器扫描实战	33	一、什么是WebDAV漏洞	42
一、什么是扫描	33	二、漏洞扫描实战	43
二、扫描实战	34	三、解决方法	43
第六招 X-scan 查看机器隐患	38	第九招 NC 监控与扫描实战	44
一、X-scan简介	38	一、监听本地计算机端口数据	44
二、X-scan安全扫描	38	二、监听远程计算机端口信息	45
三、X-scan使用技巧	39	三、将NC作为扫描器使用	45

第三章 卡卡——木马植入与防范

第十招 扫描的追踪与防范	45	二、开启远程视频	62
一、使用Internet防火墙	45	三、服务器端清除	64
二、使用扫描监测工具	46	第六招 冰河入侵与防范	64
三、让系统对Ping说“不”	47	一、木马入侵与反入侵实战	64
第十一招 图片中“捆绑”木马揭秘	50	二、反弹式木马的反入侵	67
一、图片与程序的“捆绑”	50	第七招 巧用 Port Reporter 识别木马	68
二、COPY命令也来玩捆绑	51	一、安装和卸载Port Reporter	68
三、使用专用工具玩“捆绑”	51	二、配置Port Reporter“捉”木马	69
第十二招 木马加壳与脱壳	53	三、日志文件分析	70
一、穿马甲——木马加壳的实现	53	四、根据端口查杀木马	71
二、换了马甲照样认识你——检测加壳方式	54	第八招 “微点主动防御”主动预防木马	72
三、原形毕露——脱壳实战	55	一、安装过程中的配置与更新	72
第十三招 影片木马攻防实战	56	二、安全防护，多管齐下	73
一、影片木马的特点	56	三、漏洞扫描，消除系统隐患	73
二、RM影片木马制作	57	四、主动防御，轻松截杀未知病毒木马	73
三、RM影片木马的防范	59	五、控制进程，确保安全	74
第十四招 潜藏在RMVB 影片中的网页木马	60	六、巧妙设置，自动防护	74
一、巧用RM恶意广告清除器	60	七、日志管理，了然于心	75
二、使用快乐影音播放器清除广告	61	第九招 Windows 木马清道夫斩杀木马	75
三、迅雷也能查杀弹窗广告	61	一、全方位检测木马	75
第十五招 探秘远程开启视频的木马	62	二、扫描系统漏洞	76
一、远程开启视频的意义	62	三、探测可疑模块	76
		四、监视网络连接	77



五、查看共享目录	77
第十招 DLL 木马追踪与防范	77

一、动态嵌入式DLL木马介绍	77
二、DLL木马的消除	79



第四章 杰拉德——远程控制与反控制



第一招 UltraVNC 轻松遥控远程电脑	82
一、被控端（服务器）设置	82
二、控制端（客户）设置	82
三、实现远程连接	83
第二招 巧用“网络人”随时远程控制	84
一、用远程IP和密码快速控制	84
二、用会员名和自定义密码连接	86
三、网络人电脑控制器操控远程电脑	87
第三招 WinVNC 远程控制实例	87
一、Win VNC简介	87
二、配制服务器	87
三、客户端连接	88
第四招 用 Winshell 定制服务端远程控制	88
一、WinShell简介	88
二、应用实战	88
第五招 一台电脑实现“多点”控制	90
一、QuickIP能做什么	90
二、设置服务器端	91
三、设置客户端	91

四、远程控制实战	92
第六招 Tftp 实现远程上传下载	93
一、安装Tftp服务	93
二、使用Tftp服务	94
三、防范Tftp入侵	94
第七招 巧用屏幕间谍定时抓屏监控	95
一、屏幕间谍简介	95
二、应用实战	95
第八招 灰鸽子对局域网内部远程控制	96
一、灰鸽子简介	96
二、生成服务器端	97
三、查看控制效果	98
四、卸载灰鸽子	98
第九招 监控远程服务器信息	100
一、软件简介	100
二、应用实战	100
第十招 用 Simple Bind 打造远程控制程序	101
一、合并EXE文件	101
二、修改合并后的EXE文件的图标	101



前锋：进攻！一击致命



第五章 德罗巴——网络炸弹与暴力攻击



第一招 常用初级炸弹攻防	104
一、蓝屏炸弹	104

二、Ping轰炸防范	105
三、UDP攻击	106

四、蜗牛炸弹	107	第六招 DQ 攻击溢出攻击	112
第二招 IP 炸弹工具 IP Hacker	107	一、漏洞描述	112
一、IP Hacker简介	107	二、入侵IDQ漏洞	112
二、应用实战	107	三、防范对策	113
第三招 邮箱炸弹攻防	108	第七招 RPC 溢出工具	114
一、基本应用	108	一、漏洞描述	114
二、高级应用	109	二、入侵实战	114
三、邮件炸弹的防范	110	三、防范方法	115
第四招 QQ 炸弹攻防	110	第八招 用 AtGuard 防范攻击	116
一、QQ砸门机简介	110	一、AtGuard魅力何在	116
二、软件使用	110	二、高级应用	116
三、解决方法	111	第九招 拒绝服务攻击与防范	119
第五招 MSN 消息攻击机	111	一、原理简述	119
一、应用实战	111	二、目标的确定	121
二、防范攻击	112	三、常见拒绝服务攻击工具	123
		四、拒绝服务攻击防御方法	125

第六章 梅西——系统漏洞与网站漏洞攻防

第一招 系统漏洞基本修复	128	二、漏洞利用代码实测	137
一、什么是系统漏洞	128	三、木马的利用	138
二、使用“Windows update”打补丁	128	四、漏洞的防范	138
三、轻松配置自动更新补丁	129	第六招 L-BLOG 博客提权漏洞攻防	139
四、轻松备份补丁文件	129	一、提权漏洞实战	139
第二招 Word 0Day 漏洞攻防	131	二、漏洞分析与防范	141
一、漏洞简介	131	第七招 FTP 漏洞攻防实例	144
二、漏洞攻击实例剖析	131	一、FTP入侵入门	144
三、漏洞防范	132	二、Serv-U漏洞实战	145
第三招 Excel“远程执行代码”漏洞攻防	133	三、FTP攻击防范	146
一、漏洞简介	133	第八招 PHPwind 漏洞攻防	147
二、入侵实战解析	133	一、漏洞简介	147
三、防范策略	134	二、漏洞攻击演示	148
第四招 Adobe Flash 漏洞攻防	135	三、漏洞的防范	150
一、入侵实战	135	第九招 网站数据库攻防	150
二、漏洞分析与防范	136	一、数据库简介	150
第五招 IE7 0day 漏洞攻防	136	二、下载数据库	151
一、漏洞简介	136		



后卫：防卫！转危为安



第七章 拉姆——网络盗号与防范



第一招 当心完美 QQ 大盗	154	第九招 当心黑客用偷窥者盗取 QQ ...	167
一、初识完美QQ大盗	154	一、配置“偷窥者”	167
二、QB、QQ邮件、密保一网打尽	154	二、把本机的IP更新到空间	167
三、对杀毒软件免疫	155	三、发送服务端给被攻击者	168
第二招 QQ 强制视频聊天与防护	155	四、捕获肉鸡	168
一、强制视频聊天解析	155	第十招 多管齐下保护 QQ 安全	169
二、防范方法	156	一、防范QQ被盗8项“注意”	169
第三招 识破 QQ “假” 密码保护	156	二、QQ安全卫士——QQKeeper	169
一、认识“QQ密码反保精灵”	156	三、噬菌体密码防盗专家	170
二、防范方法	157	第十一招 防范 MSN 密码被盗取	171
第四招 轻松突破 QQ 密码保护	157	一、Msn Messenger Hack盗取密码	171
一、木马客户端制作	157	二、MessenPass查看密码	172
二、轻松盗取QQ密码	158	第十二招 MSN 精彩攻防战	173
三、轻松突破密码保护	158	一、局域网内的MSN攻击	173
四、巧用QQ申诉信息“夺取”QQ号 ..	158	二、针对外网的MSN攻击	173
第五招 QQ 聊天记录泄秘	159	第十三招 Foxmail 账户破解与防范 ...	175
一、QQ记录管家“偷窥”聊天记录 ...	159	一、邮箱使用口令的安全防范	175
二、应对策略	160	二、邮箱账户密码的防范	176
第六招 防范 QQ 密码本地破解	160	第十四招 防范邮箱账户欺骗	177
一、防范“QQ破密使者”盗取QQ	161	一、邮箱账户伪造揭秘	177
二、“密码使者”截获登录窗口中的QQ	162	二、隐藏邮箱账户	177
第七招 当心在线破解 QQ 密码	163	三、垃圾邮件的防范	178
一、在线破解QQ揭秘	163	四、重要邮箱的防范之道	181
二、“QQ机器人”盗号也疯狂	163	五、查找伪造邮箱账户的发件人	181
第八招 QQ 密码远程盗取	165	第十五招 拒绝盗号 工具软件为你护航	181
一、来自“QQ枪手”的攻击	165	一、网游保镖为你护航	182
二、防范“QQ掠夺者”盗取QQ	165	二、奇虎360保险箱保护账号	183

 第八章 拉莫斯——病毒查杀与防范

第一招 卡巴斯基全功能软件 2009 ...	186	第六招 巧用数字签名揪出可疑文件...	200
一、卡巴斯基的安装与激活	186	第七招 不用“杀软”可疑文件在线“定罪”	201
二、恶意软件主动防御	187	一、可疑文件上传检测	202
三、虚拟键盘保障网络安全	188	二、查看扫描结果	202
四、处理垃圾邮件、网页广告	188	第八招 安全护盾保护系统、文件安全	203
五、应用程序过滤保障系统安全	189	一、查杀流氓软件	203
六、轻松修复系统漏洞	190	二、危险程序轻松拦截	204
第二招 360 杀毒软件免费杀毒	191	三、重要文件全力保护	204
一、360杀毒软件安装与配置	191	四、众多安全辅助工具	205
二、实时保护系统	191	第九招 守护电脑的“看家狗”	206
三、多种方式扫描病毒	192	一、“看家狗”实时监控进程	206
四、快速修复实时保护	193	二、保护电脑中的杀毒软件	206
第三招 “小红伞”保护你的电脑.....	193	三、“看家狗”监控功能实测	207
一、自动更新病毒库	194	第十招 墨者安全专家为电脑护航.....	208
二、强大的病毒查杀能力	194	一、全局掌控墨者安全中心	208
三、出色的实时防护	195	二、权限控制墨者独创“革离术”	208
第四招 USB 全面监控防病毒	196	三、免费杀毒实时监控	209
一、U盘病毒彻底免疫	196	四、漏洞修复隐私清理	209
二、U盘读写控制轻松掌控	197	第十一招 Outpost 防火墙捍卫安全 ...	210
三、U盘监视铁证如山	197	一、设置应用程序访问规则	210
第五招 用 Syscheck 清理病毒木马 ...	198	二、轻松查杀间谍软件	211
一、根据进程识别木马	198	三、防火墙防护模式选择	211
二、一键操作快速净化	199	四、特色功能——插件扩展	212
三、停止木马服务	199	五、设置密码保护	212

 第九章 特里——网络提权与网吧攻防

第一招 轻松突破上网限制.....	214	第二招 提升网络资源下载权限.....	218
一、突破局域网上网封锁	214	一、加密式的Flash动画下载	219
二、使用工具搜索代理服务器	215	二、使用站点资源探测器下载	220

三、通过IE临时文件夹破解	220	一、破解工具解除网吧的下载限制	227
四、FlashGet添加代理突破下载限制	221	二、使用“2008网吧破解程序”	228
五、下载在线流媒体	222	三、找出作祟的网管软件	228
第三招 BT 下载的限制与突破	223	四、将网吧电影带回家	229
一、限制内网BT下载	223	第六招 网吧常见攻击与防范	230
二、突破端口封锁玩BT	226	一、局域网攻击原理	230
第四招 在线解除网吧下载限制	226	二、局域网终结者	230
一、网吧限制的“表面文章”	226	第七招 ARP 攻防实例解析	231
二、利用网站在线解除限制	227	一、欺骗原理	231
第五招 使用工具解除网吧限制	227	二、欺骗实例	232
		三、ARP欺骗防范	233

第十章 赞布罗塔——数据的加密与解密

第一招 电脑系统另类加密	236	第七招 打造免费的 U 盘加密	245
一、用U盘“开机”	236	一、快速移动加密	246
二、独一无二的面孔加密术	237	二、强度压缩加密	246
第二招 巧用图片进行另类加密	238	第八招 对电脑中的特定程序加密	247
一、用图片隐藏机密文本信息	238	一、设置密码	247
二、图片加密管理好帮手	239	二、限制特定程序的运行	247
第三招 文件分割巧加密	240	三、文件/文件夹加密	248
一、分割文件	240	四、锁定其他选项	248
二、合并文件	240	第九招 巧用软件杜绝 Word 文档泄密	249
第四招 文件隐藏巧加密	241	一、分析Word文档的隐私信息	249
一、创建隐藏文件夹	241	二、彻底清除Word文档隐私	250
二、操纵“隐藏文件夹”	241	第十招 当心系统缓存泄露你的秘密	251
三、编辑和删除隐藏文件夹	242	一、轻松查看邮件附件	251
四、文件隐藏大师设置	242	二、邮件正文也手到擒来	251
第五招 WinRAR 的“另类”加密方法	243	三、堵住漏洞，预防为先	252
一、利用MP3巧加密	243	第十一招 加密奇兵保护重要资料	253
二、让加密文件更安全	244	一、常规加密	253
第六招 别具特色的分时段加密	244	二、隐藏加密	254
一、添加加密用户	244	三、程序加锁	255
二、加密文件夹	244	第十二招 虚拟磁盘彻底隐藏你的隐私	256
三、设置自解密时间	245	一、创建虚拟加密磁盘	256
四、激活加密功能	245	二、虚拟磁盘的使用	257

第十三招 常用网络登录密码解除..... 258

- 一、找回“自动完成”密码 258
- 二、用黑雨密码探测器恢复邮箱密码 ... 259
- 三、巧用MessenPass查看MSN密码 259

第十四招 压缩文档解密..... 260

- 一、用RAR PassWord Cracker恢复RAR密码 260
- 二、“多功能密码破解软件”恢复密码 261

**守门：不可逾越的防线****第十一章 布冯——网络安全终极防范****第一招 隐藏 IP 增强安全 264**

- 一、为什么要隐藏IP 264
- 二、以假乱真藏IP 265
- 三、修改注册表藏IP 265
- 四、使用代理藏IP 265
- 五、使用提供匿名冲浪的网站隐藏IP ... 266
- 六、Telnet入侵时隐藏IP 266
- 七、使用工具软件藏IP 266
- 八、验证IP是否隐藏成功 267

第二招 巧施妙招防范挂马网站..... 268

- 一、金山网盾识别恶意网页 268
- 二、Mcafee安全工具检测网站安全 269

第三招 无线网络安全防范..... 270

- 一、无线WEP加密方法 271
- 二、轻松获取WEP密码 271
- 三、破解无线WEP加密 272

第四招 多种手段保护隐私..... 275

- 一、清除操作“痕迹”基本功 275
- 二、Cookies安全管理..... 276
- 三、让隐私数据无从恢复 277
- 四、短暂离开的防护措施 278

第五招 一键 GHOST 恢复系统 279

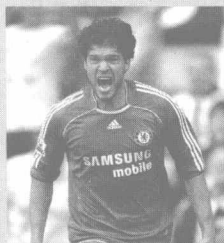
- 一、软件安装 279
- 二、系统备份 280
- 三、一键手动备份 281
- 四、系统恢复 281
- 五、高级功能 282

第六招 用影子系统为电脑安装“防护罩” 282

- 一、最有名的影子系统Power Shadow ... 282
- 二、数据保护“伞” Shadow User 283
- 三、Returnil虚拟影子系统..... 285

第七招 卷影副本让 Vista 完好如初 ... 285

- 一、开启系统还原 285
- 二、灵活选择备份文件 286
- 三、体验卷影副本的功效 287



球星小档案

姓名：巴拉克

国籍：德国（国家队队长、灵魂）

身高：189CM

生日：1976年9月26日

球员身价：1200万欧元

最擅长位置：后腰、中前卫

现效力俱乐部：英格兰超级联赛——切尔西

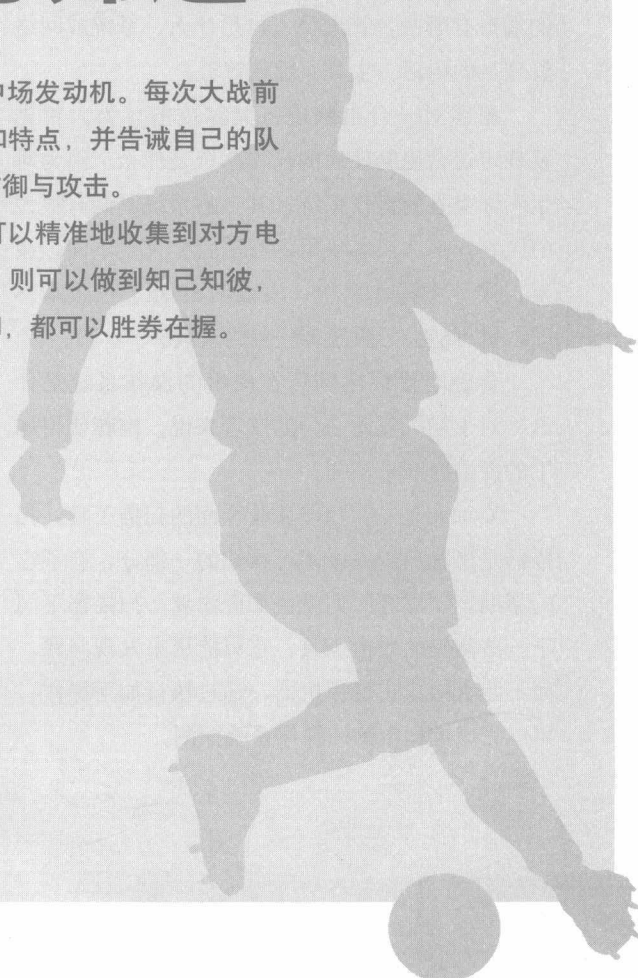
CHAPTER 01

巴拉克（收集对手信息，从容应对）

信息搜集与筛选

巴拉克，德国国家队队长，标准的中场发动机。每次大战前总能精准地收集到对方球员的准确信息和特点，并告诫自己的队友根据对手的习性特点进行有针对性的防御与攻击。

在网络黑客攻防中更是如此，如果可以精准地收集到对方电脑的相关信息，查找和跟踪对方的电脑，则可以做到知己知彼，打有准备之仗。这样无论是攻击还是防御，都可以胜券在握。





第一招 巧用X-scan探测系统版本

每次足球比赛前，足球队员和教练组都要详细地收集对方队员的资料和信息。只有全面了解了对方的信息资料才可以有针对性的破解对方攻击，掌握球场上的主动。

黑客界同样如此：无论目标的规模有多大，安全防范有多严密，只要是人类参与设计及管理，那么人为因素产生的安全问题就一定存在。黑客在执行任务前的信息搜集，就是用于找出这些安全问题。在执行黑客任务之前，应尽量多收集一些关于目标电脑的信息，这些信息主要包括安装的是什么操作系统，提供了哪些服务，开放的端口有哪些，管理员入口是什么，系统或网络管理员的电话、生日、姓名等等。

黑客对一台电脑进行黑客攻击行为，首先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的区别，那么黑客使用的方法就会完全不同。甚至，同一类操作系统，安装的SP补丁包版本不同，也可能会导致黑客任务的失败。

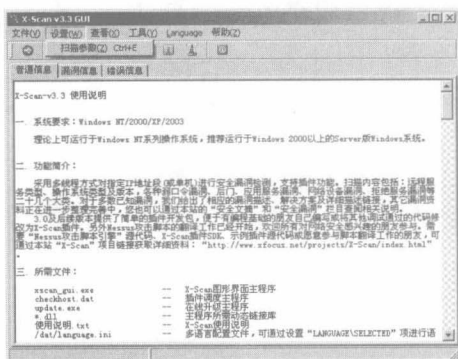
要确定目标电脑正在使用的操作系统是什么，对于初入安防之门的读者来说，推荐使用如下探测方法来获知。

X-Scan是一款功能比较全面的扫描工具，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。

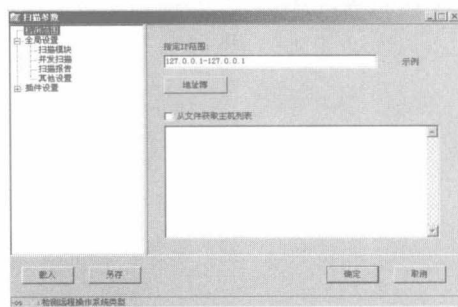
一、设置扫描参数

【第1步】首先，至国内的著名安全网站“安全焦点”下载X-Scan 中文版。

【第2步】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。



【第3步】依次单击“设置”→“扫描参数”菜单，在弹出的下图所示对话框中，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。



【第4步】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。



二、开始扫描

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。



三、查看操作系统版本

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：个人电脑一般是安装Windows XP或Vista。



第二招 用Ping命令探测网络连接

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。

一、Ping命令参数介绍

Ping命令的参数作用解释如下：

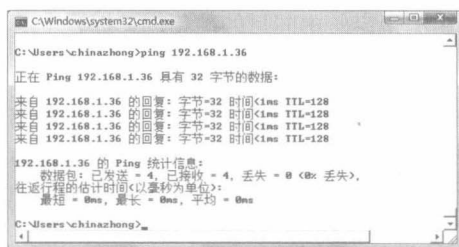
-t：不断使用Ping命令发送回响请求信息到目的地。要中断并退出Ping，只需按“Ctrl+C”键。初级黑客常喜欢使用这个参数对目标电脑进行攻击。

-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须是直接可达的(必须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指定的回响请求消息。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。

二、Ping命令探测实例

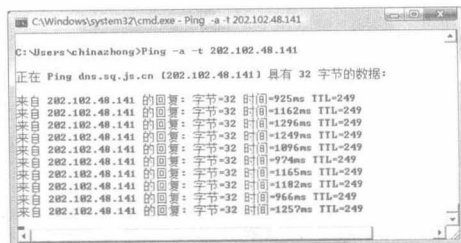
下面给出一些Ping命令的典型使用方法。

1. 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,所以能通过此命令来检查本机的网卡驱动。

2. 实例2: 多参数合用检测

假设,现在使用“Ping -a -t 202.102.48.141”命令对IP地址为202.102.48.141的计算机进行探测,可以得到如图所示的反馈信息。



通过反馈信息,可以得知上述命令中的参数“-a”检测出了该机的Net BIOS名为dns.sq.js.cn;参数“-t”在不断向该机发送数据包。

通常,Ping命令会反馈如下两种结果:

结果1: 请求超时

这表示没有收到网络设备返回的响应数据包,也就是说网络不通。出现这个结果原因很复杂,通常有如下几种可能:

- * 对方装有防火墙并禁止ICMP回显。
- * 对方已经关机。
- * 本机的IP设置不正确或网关设置错误。
- * 网线不通。

结果2: 来自 202.102.*.141 的回复: 字节=32 时间<1ms TTL=128

这表示网络畅通,探测使用的数据包大小为32Bytes,响应时间小于1ms。TTL这个值需要细说一下,TTL全称“Time To Live”,中文意思