

黑客高手
技术档案

完全掌握

黑客攻防

实战超级手册

深入内涵，全盘理解，掌握精髓

- 洞察黑客入侵伎俩和攻击手段，掌握黑客防范技术和方法，确保信息安全
- 知己知彼，方能百战不殆

DVD

7小时

多媒体视频讲解

武新华 王英英 安向东等 编著



机械工业出版社
China Machine Press



完全掌握

黑客攻防

实战超级手册

武新华 王英英 安向东 等编著



机械工业出版社
China Machine Press

本书从了解黑客攻击手段,达到完全掌握防范黑客攻击为目的。全书以“攻”、“防”两个不同的角度,介绍黑客攻击手段的同时,讲述相应的防范技术;通过模拟案例,图文并茂地再现了黑客入侵网络与防御的全过程。书中主要内容包括:黑客入侵准备、基于系统漏洞的入侵与防范、局域网攻防实例、QQ 攻防实例、邮件欺骗与轰炸、密码攻防实例、网游与网吧攻防实例、手机病毒防范与清除、网银炒股安全实战、网站、数据库与服务器攻防、揭秘留后门与清脚印伎俩、揭秘自行制造病毒、解密黑客入侵与检测、备份升级与数据恢复、网络安全与防范。

本书突出任务驱动与案例教学,并配合长达7小时的多媒体视频教学,适合具有一定安全基础知识和工具使用基础的读者、网络管理人员、黑客技术爱好者阅读和参考。

封底无防伪标均为盗版

版权所有,侵权必究

本书法律顾问 北京市展达律师事务所

图书在版编目(CIP)数据

完全掌握黑客攻防实战超级手册/武新华,王英英,安向东等编著. —北京:机械工业出版社,2010.5

ISBN 978-7-111-30361-9

I. ①完… II. ①武… ②王… ③安… III. ①计算机网络—安全技术—手册 IV. ①TP393.08-62

中国版本图书馆CIP数据核字(2010)第064418号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑:夏非彼 迟振春

北京科普瑞印刷有限责任公司印刷

2010年5月第1版第1次印刷

188mm×260mm • 30.5印张

标准书号:ISBN 978-7-111-30361-9

ISBN 978-7-89451-490-5(光盘)

定价:58.00元(附1DVD)

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

客服热线:(010) 88378991; 82728184

购书热线:(010) 68326294; 88379649; 68995259

投稿热线:(010) 82728184; 88379603

读者信箱:booksaga@126.com

本书从了解黑客攻击手段，达到掌握防范黑客攻击为目的。全书围绕“攻”、“防”两个不同的角度，介绍黑客攻击手段的同时，讲解了相应的防范方法；通过模拟案例，图文并茂地再现了黑客入侵网络与防御的全过程。

本书内容

- 介绍黑客攻击入侵手段与具体防范的方法和技巧，通过典型生动的案例向读者展示了多种黑客破坏性的攻击方法和工具的使用；
- 以深入剖析黑客入侵过程为主线来展开全书内容，向读者讲述入侵者是如何实现信息的搜集；
- 告知黑客是如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马等入侵手段）；
- 介绍黑客是如何实现入侵，即远程连接，入侵后如何执行各种任务；
- 讲解黑客是如何留下后门达到再次进入系统的目的；入侵者如何清除系统日志防止目标服务器发现入侵的痕迹。

本书最主要的精髓在于知己知彼，方能百战不殆。希望读者能够运用书中所揭示的黑客攻击防守方法去了解黑客，进而达到防范黑客攻击的目的，使自己的网络系统更加安全、稳固。

注 意：书中所有实例写作是在一个模拟的局域网内调试通过的。

本书特色

本书以场景式教学、案例驱动与任务进阶为写作特色，在书中可以看到一个个生动的场景案例。通过完成一个个任务的实践，读者不仅可以轻松掌握有关网络安全知识，还可在不知不觉中快速提升网络安全防范的实战技巧。

- 场景式教学：紧扣“理论+实战，图文+视频=全面提升学习效率”的主导思想，采用最为通俗易懂的图文解说，为读者展示操作流程。
- 案例驱动：盘点最新黑客技术，并采用你攻我守的方法详述范例完整操作过程，便于读者实战演练。
- 任务进阶：详细分析每一个黑客入侵步骤，推断入侵者的每一入侵步骤的目的及所要完成的任务，并对入侵中的主要问题作必要的说明与解答。

每个专题都涉及黑客的攻击手段、造成的严重后果，以及如何预防，使其转危为安，最终挽回损失。每个专题给出具体案例，都是耳熟能详且

与现实生活息息相关的典型代表。

读者对象

本书涉及面较广，可作为一本黑客攻防技术的速查手册，也适合如下读者学习使用：

- 网络管理人员；
- 喜欢研究黑客技术者；
- 系统维护人员和电脑爱好者；
- 大中专院校相关专业的学生。

增值服务

随书附赠的 DVD 光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过增加读者对主流操作手法感性的认识，使读者提高防范技能，确保自己的系统安全。

此外，如发现本书中有不妥或需要改进之处，还可通过访问 <http://www.newtop01.com> 与笔者进行沟通，并真心希望和广大读者互动的过程中能得到提高。

本书编者

本书作者长期从事网络安全管理工作，具有较强的实践操作能力及一线拼杀经验，可带领广大技术者穿越迷雾，把黑客们的伎俩侦察得清清楚楚。在本书的编写中：冯世雄负责第 1 章，张晓新负责第 2 章，陈艳艳负责第 3 章，李防负责第 4 章，余建国负责第 5、6 章，王肖苗负责第 7 章，孙世宁负责第 8 章，杨平负责第 9 章，段玲华负责第 10 章，李伟负责第 11 章，王英英负责第 12 章，郑静负责第 13 章，刘双红负责第 14 章，安向东负责第 15 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有失误、遗漏之处，我们心存谨敬，随时恭候您提出宝贵意见。

最后，需要提醒读者的是：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，否则后果自负。

编者

2010.04



目 录

前 言

第 1 章 黑客入侵准备	1
1.1 探测操作系统	2
1.1.1 使用 X-Scan 探测	2
1.1.2 使用 Ping 命令探测	3
1.1.3 通过网站探测	5
1.2 探测网站信息	6
1.2.1 探测域名和 IP	6
1.2.2 探测网站注册信息	9
1.3 探测搜索引擎	11
1.4 筛选信息	12
1.4.1 人工筛选	12
1.4.2 软件筛选	13
1.5 监听网络	15
1.5.1 监听实战	15
1.5.2 网络监听防范方法	20
1.6 扫描与嗅探实例分析	20
1.6.1 Sss 扫描器	20
1.6.2 流光扫描工具	26
1.6.3 Nmap 嗅探器	28
1.6.4 Iris 嗅探器	29
1.7 黑客常见问题解答	32
第 2 章 基于系统漏洞的入侵与防范	33
2.1 Windows 系统的安全隐患	34
2.1.1 Windows 系统中的漏洞产生原因	34
2.1.2 Windows 系统中的常见漏洞	34
2.2 系统漏洞攻击	39
2.2.1 解析 139 端口漏洞的攻击与防范	39
2.2.2 解析 SAM 数据库安全漏洞的攻击与防范	41

2.2.3	解析 Windows XP 热键漏洞的攻击与防范	43
2.3	Unicode 漏洞攻击	44
2.3.1	利用扫描软件查找 Unicode 漏洞	44
2.3.2	利用 Unicode 漏洞攻击目标计算机	45
2.3.3	利用 Unicode 漏洞控制目标主机	49
2.3.4	防范 Unicode 漏洞的措施	49
2.4	远程缓冲区溢出漏洞攻击	50
2.4.1	缓冲区溢出原理	50
2.4.2	缓冲区溢出漏洞的攻击方式	51
2.4.3	缓冲区溢出漏洞的防范方式	52
2.5	黑客常见问题解答	53
第 3 章	局域网攻防实例	54
3.1	Windows XP 安全共享	55
3.1.1	禁用简单文件共享	55
3.1.2	创建用户账户和组用户	56
3.1.3	设置共享文件	59
3.1.4	设置共享权限	61
3.1.5	修改组策略	61
3.1.6	封杀系统默认共享	63
3.2	Windows Vista 安全共享	67
3.3	共享漏洞攻击实例	69
3.3.1	使用工具	69
3.3.2	配合 IPC\$	70
3.3.3	窃取共享密码	72
3.4	共享漏洞防范措施	73
3.4.1	配置安全策略	74
3.4.2	设置与管理权限	75
3.5	黑客常见问题解答	79
第 4 章	QQ 攻防实例	80
4.1	常见的攻击与防范方式	81
4.1.1	QQ 信息炸弹的攻击与防范	81
4.1.2	QQ 远控精灵的攻击与防范	83
4.1.3	QQ 聊天记录的泄密与防范	84
4.2	QQ 聊天记录的查看与保护	84

4.2.1	QQ 聊天记录器.....	85
4.2.2	QQ 聊天记录终结者.....	86
4.2.3	QQ 聊天记录查看器.....	87
4.2.4	QQ 聊天记录保护方法.....	89
4.3	警惕“QQ 密保大盗”	91
4.3.1	木马客户端制作分析	92
4.3.2	盗取 QQ 密码解析.....	92
4.3.3	突破密码保护.....	93
4.3.4	通过 QQ 申诉信息夺回 QQ 号.....	93
4.4	警惕“QQ 大杀器”	96
4.4.1	QQ 号盗取剖析.....	96
4.4.2	自动生成 QQ 尾巴.....	97
4.4.3	自动弹出网页.....	98
4.5	QQ 安全的防范措施.....	99
4.5.1	防范 QQ 被盗的 8 个“注意”事项.....	99
4.5.2	QQ 密码防盗专家.....	104
4.5.3	QQ 安全卫士.....	106
4.5.4	QQ 医生.....	107
4.6	全面打造安全 QQ.....	110
4.6.1	利用磁盘读写权限封杀 QQ 广告.....	110
4.6.2	为 QQ 硬盘设置密码.....	111
4.6.3	为 QQ 通讯录设置密码.....	112
4.6.4	保护 Q 币.....	112
4.7	黑客常见问题解答.....	113
第 5 章 邮件欺骗与轰炸.....		115
5.1	破解邮箱密码.....	116
5.1.1	邮箱暴力破解的原理	116
5.1.2	邮箱暴力破解的方式	116
5.2	获取邮箱密码的欺骗手段.....	120
5.2.1	了解电子邮件欺骗的手段	120
5.2.2	邮件地址欺骗获.....	121
5.2.3	Outlook Express 欺骗.....	122
5.2.4	TXT 文件欺骗.....	126
5.2.5	绕过 SMTP 服务器欺骗.....	127
5.3	攻击邮箱的方式.....	128

5.3.1	电子邮箱炸弹的原理	128
5.3.2	电子邮箱炸弹的攻击方法	129
5.3.3	电子邮箱炸弹的防范及垃圾邮件过滤	131
5.4	邮件安全的防范措施	135
5.4.1	禁止 HTML 格式邮件的显示	136
5.4.2	修改文件的关联性	136
5.4.3	加密自己的邮箱账户	137
5.5	黑客常见问题解答	138
第 6 章	密码攻防实例	140
6.1	系统密码攻防	141
6.1.1	Syskey 的双重加密与解密	141
6.1.2	BIOS 密码的设置与解除	142
6.1.3	系统的登录密码设置	146
6.1.4	找回 Windows XP 的管理员密码	149
6.1.5	利用 ERD 恢复系统密码	152
6.1.6	系统其他的密码设置	154
6.2	文件和文件夹密码攻防	160
6.2.1	NTFS 文件系统加密数据	160
6.2.2	文件夹加密大师	161
6.2.3	图片加密好帮手	165
6.2.4	文件分割巧加密	166
6.2.5	“机器虫”加密软件	167
6.2.6	WinGuard 加密应用程序	168
6.3	办公文档密码攻防	169
6.3.1	Word Key 密码恢复工具	170
6.3.2	AOPR 破解工具	171
6.4	压缩文件密码攻防	172
6.4.1	RAR Password Cracker 恢复密码	172
6.4.2	暴力破解压缩文件密码	174
6.5	黑客常见问题解答	175
第 7 章	网游与网吧攻防实例	176
7.1	网络游戏“盗号”大揭秘	177
7.1.1	防范利用木马盗号	177
7.1.2	防范利用远程控制方式盗号	180
7.1.3	防范利用系统漏洞盗号	183

7.2	网站充值骗术大揭秘.....	184
7.2.1	欺骗原理.....	184
7.2.2	防范方法.....	184
7.3	CS 作弊器大揭秘.....	186
7.3.1	作弊器的分类.....	186
7.3.2	作弊器的防范.....	187
7.4	服务器遭受 DoS 攻击大揭秘.....	187
7.4.1	DoS 攻击的工具.....	187
7.4.2	攻击 CS 服务器的解析.....	191
7.4.3	DoS 攻击的防范方法.....	191
7.5	利用内存补丁破解传奇外挂.....	192
7.5.1	外挂介绍.....	192
7.5.2	外挂验证.....	193
7.6	网游外挂大揭秘.....	196
7.6.1	动作式外挂.....	197
7.6.2	木马式外挂.....	198
7.6.3	加速式外挂.....	200
7.6.4	封包式外挂.....	201
7.7	局域网监听大揭秘.....	205
7.7.1	监听的原理.....	205
7.7.2	监听的防范方法.....	206
7.8	本地账号破解大揭秘.....	208
7.8.1	“自动记住密码”的危害.....	208
7.8.2	破解账号的防范方法.....	212
7.9	网游盗号木马大揭秘.....	212
7.9.1	容易被捆绑木马的程序.....	213
7.9.2	木马程序的感染途径.....	214
7.9.3	容易被盗的网游账号.....	215
7.10	黑客常见问题解答.....	219
第 8 章	手机病毒防范与清除.....	220
8.1	手机病毒的来源.....	221
8.2	手机病毒的传染途径.....	222
8.2.1	网络下载.....	222
8.2.2	红外或蓝牙传输.....	222
8.2.3	短信与乱码传播.....	223

8.3 手机病毒的特点	223
8.3.1 手机中病毒的症状	223
8.3.2 手机中病毒的种类	224
8.3.3 手机病毒的攻击对象	225
8.4 手机病毒的防范建议	226
8.5 手机病毒的常见清除方法	227
8.6 黑客常见问题解答	231
第9章 网银炒股安全实战	232
9.1 网上交易中的安全防范	233
9.1.1 网银常见攻击手段	233
9.1.2 网银攻击防范技巧	237
9.1.3 网银安全防范工具	241
9.1.4 网络钓鱼防范工具	247
9.2 网络炒股中的安全防范	252
9.2.1 网上炒股安全概述	252
9.2.2 利用杀毒软件预防	253
9.2.3 利用“股票安全防盗系统”预防	257
9.3 黑客常见问题解答	260
第10章 网站、数据库与服务器攻防	261
10.1 网站攻击	262
10.1.1 常见的攻击手段	262
10.1.2 管理员入口入侵	263
10.1.3 网页木马入侵	266
10.1.4 网站漏洞分析	268
10.1.5 网站的防范方法	275
10.2 数据库攻防	276
10.2.1 防范利用下载数据库进行攻击	276
10.2.2 防范利用 SQL Server 进行攻击	278
10.2.3 防范利用专用工具进行攻击	282
10.2.4 防范利用源代码分析进行攻击	284
10.2.5 防范数据库攻击的秘技	286
10.3 服务器攻防	289
10.3.1 漏洞入侵与防御	289
10.3.2 服务器软件入侵与防御	293



10.3.3	账户入侵与防御	300
10.4	黑客常见问题解答	305
第 11 章	揭秘留后门与清脚印	306
11.1	账号后门	307
11.1.1	手工克隆账号	307
11.1.2	在命令行下制作后门账号	311
11.2	漏洞后门	313
11.2.1	制造 Unicode 漏洞	313
11.2.2	制造 .idq 漏洞	314
11.2.3	制造系统服务漏洞后门	314
11.3	木马后门	318
11.3.1	wolf	318
11.3.2	SQL 后门	322
11.4	清除日志	323
11.4.1	利用手工清除日志	323
11.4.2	利用工具清除日志	325
11.5	黑客常见问题解答	326
第 12 章	揭秘自行制造病毒	327
12.1	借助代码制造病毒	328
12.1.1	VBS 脚本病毒生成机	328
12.1.2	VBS 蠕虫制造机	332
12.1.3	VBS 脚本病毒	335
12.2	不借助宏制造 Word 病毒	340
12.2.1	MS06-027 漏洞	340
12.2.2	MS05-016 漏洞	341
12.2.3	普通 Word 文档病毒	342
12.2.4	功能更强大的 Word 病毒	345
12.3	借助 U 盘入侵整个办公网	347
12.3.1	自己制造 U 盘病毒	347
12.3.2	多重加壳免杀 U 盘病毒	348
12.3.3	北斗压缩二次加壳	349
12.3.4	使用闪盘窥探者	351
12.3.5	U 盘病毒的防范方法	352
12.4	黑客常见问题解答	356

第 13 章 解密黑客入侵与检测	358
13.1 思易 ASP 木马追捕	359
13.2 萨客嘶入侵检测系统	360
13.2.1 萨客嘶入侵检测系统的设置	360
13.2.2 萨客嘶入侵检测系统的使用	364
13.3 利用 IIS Lockdown Tool 检测网站安全	366
13.4 单机版极品安全卫士 Cather	370
13.5 入侵检测系统 BlackICE	375
13.6 路由安全检测 SolarWinds	379
13.7 使用网络安全特警防止黑客入侵	380
13.8 黑客常见问题解答	391
第 14 章 备份升级与数据恢复	392
14.1 数据备份与升级概述	393
14.1.1 什么是数据备份	393
14.1.2 什么是系统升级	395
14.1.3 数据备份实例演示	396
14.2 恢复硬盘数据	401
14.2.1 造成数据丢失的原因	401
14.2.2 使用和维护硬盘的注意事项	401
14.2.3 数据恢复工具 Easy Recovery 和 Final Data	402
14.3 备份与恢复 Windows XP 操作系统	407
14.3.1 使用 Drive Image 备份/还原操作系统	408
14.3.2 利用系统自带的还原功能	411
14.3.3 利用 Ghost 实现系统备份还原	414
14.4 备份与恢复 Windows Vista 操作系统	416
14.4.1 Windows Vista 自带的备份/还原功能	416
14.4.2 利用安装文件备份恢复 Windows Vista 系统	419
14.5 备份与还原其他资料	421
14.5.1 备份还原驱动程序	421
14.5.2 备份还原注册表	423
14.5.3 备份还原病毒库	424
14.5.4 备份还原收藏夹	425
14.5.5 备份还原电子邮件	427
14.6 黑客常见问题解答	429

第 15 章 网络安全与防范	430
15.1 360 安全卫士.....	431
15.1.1 系统漏洞修复.....	431
15.1.2 恶意软件查杀.....	433
15.1.3 系统诊断与修复.....	435
15.1.4 病毒查杀.....	437
15.2 金山系统清理专家.....	440
15.2.1 恶意软件查杀.....	440
15.2.2 浏览器修复.....	442
15.2.3 进程和启动项管理.....	443
15.2.4 历史痕迹清理.....	444
15.2.5 特色功能.....	445
15.3 瑞星杀毒软件.....	447
15.3.1 全新的脱壳功能.....	447
15.3.2 开机“抢先”杀毒.....	448
15.3.3 独特的“碎甲”技术.....	449
15.3.4 主动扫描、修复漏洞.....	449
15.3.5 嵌入式查杀病毒.....	450
15.4 U 盘病毒防护盒.....	451
15.4.1 拦截免疫.....	451
15.4.2 创建 Autorun.inf 文件实现 U 盘免疫.....	452
15.4.3 强力修复功能.....	452
15.4.4 强大的进程管理.....	454
15.5 PeerGuardian 软件.....	455
15.5.1 PeerGuardian 的安装设置.....	456
15.5.2 阻止 P2P 中的可疑连接.....	458
15.5.3 PeerGuardian 的优化设置.....	459
15.6 Net Tools X 工具.....	460
15.6.1 进程管理.....	461
15.6.2 Ping 探测.....	461
15.6.3 局域网安全管理.....	462
15.6.4 网络连接管理.....	463
15.6.5 地址转换管理.....	465
15.7 数字签名功能.....	466
15.7.1 查看文件的数字签名.....	466
15.7.2 结合时间找到可疑的病毒文件.....	467

第 1 章

黑客入侵准备

重点提示

- 探测操作系统
- 探测网站信息及搜索引擎
- 扫描和嗅探实例分析

本章精粹

本章主要介绍黑客入侵前的准备工作；黑客入侵成功与否都不是偶然的，在入侵前的准备工作将直接影响着入侵的结果。入侵前的准备工作包括：探测系统、网站信息探测、搜索引擎探测、信息的筛选、网络监听与嗅探等，所以读者了解此内容后，可提早对黑客进行防范。

通常情况下,黑客在进行攻击之前都需要对目标进行全方位分析,当分析出的数据达到攻击条件之后,黑客便会主动攻击,并会在最短时间内攻破目标。因此,黑客攻击前的信息搜集的工作是最重要的,往往需要几个小时甚至几十个小时,越成熟的黑客在信息搜索上花费的时间就越多,攻击成功的几率也就越大。

1.1 探测操作系统

当黑客确定一个攻击目标时,首先会收集该目标电脑的信息,其中包括:安装的操作系统、启用的服务、开放的端口、管理员登录口,甚至有时还需要调查系统或网络管理员的私人信息,如电话、生日、姓名等。在收集信息时先要确定对方的操作系统,因为对于不同类型、不同版本的操作系统,系统漏洞区别很大,直接关系到黑客攻击时所使用的方法。此外,同一类型及版本的操作系统,由于安装的补丁包版本的不同,也决定着黑客攻击的失败与否。下面介绍几种适合防范者掌握的黑客使用的探测方法,帮助大家及早防范黑客入侵。

1.1.1 使用 X-Scan 探测

X-Scan 是一款扫描软件,可采用多线程方式对指定单机或 IP 地址段进行漏洞扫描,也支持插件功能。它基于图形界面与命令行两种操作方式,直观明了、简单易学。

下面以 X-Scan v3.3 为例介绍其具体的操作步骤:

Step 01 双击“X-Scan”应用程序,即可打开【X-Scan v3.3】主窗口,在【普通信息】选项卡中显示了该软件的使用说明,如图 1-1 所示。

Step 02 选择【设置】→【扫描参数】菜单项,即可打开【扫描参数】对话框,在其中选择【检测范围】选项,在右侧设置面板中指定要扫描目标计算机的 IP 地址,如图 1-2 所示。

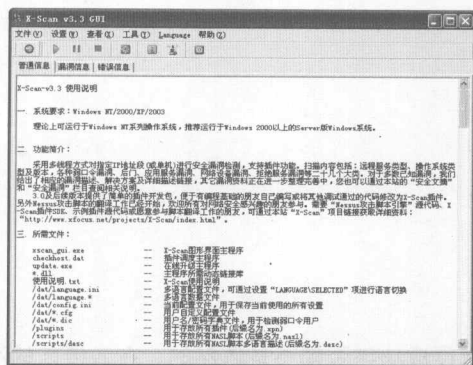


图 1-1 【X-Scan v3.3】主窗口

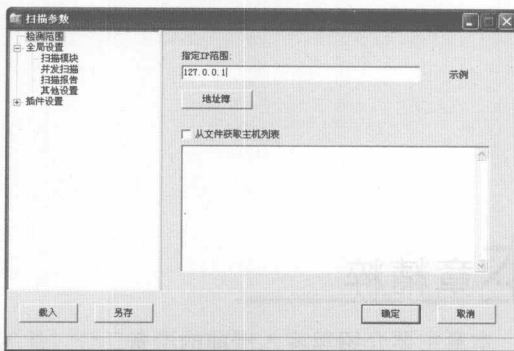


图 1-2 设置【检测范围】

Step 03 依次展开【全局设置】→【扫描模块】选项,在中间的设置面板中勾选“远程操作系统”复选框,如图 1-3 所示。

Step 04 选择【扫描报告】选项,即可在右侧设置面板中选择报告结果的方式。报告文件的生成方式有两种:HTML 文件和 TXT 文件,可根据情况进行选择,如图 1-4 所示。