

网络安全技术应用丛书

畅销书《杀破狼》作者团队最新力作!

铜墙铁壁

——黑客防范技巧与工具

武新华 刘岩 段玲华 等编著

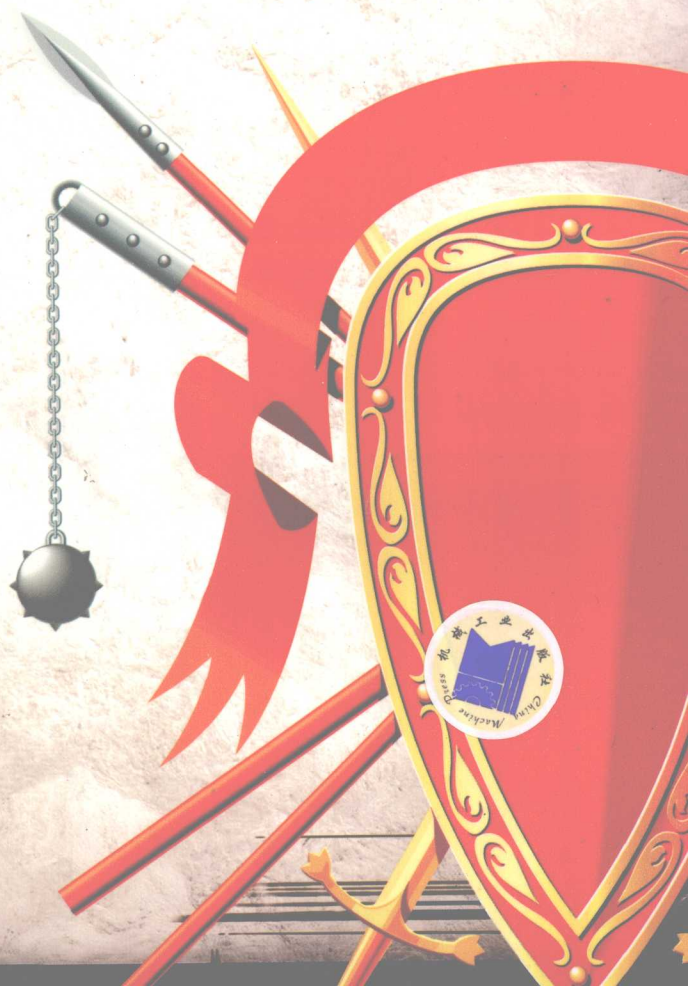
- ◆ Windows系统漏洞及防范措施
- ◆ 木马和间谍软件的伪装与查杀
- ◆ Web攻防实战演练
- ◆ 电子邮件攻防实战
- ◆ 后门与自身防护技术
- ◆ 网络代理与恶意进程清除
- ◆ 数据备份与恢复
- ◆ 打好网络安全防御战



附赠超值多媒体语音光盘



机械工业出版社
CHINA MACHINE PRESS



网络安全技术应用丛书

铜墙铁壁——黑客防范技巧与工具

武新华 刘岩 段玲华 等编著



机械工业出版社

本书紧紧围绕黑客防范技巧与工具展开，在剖析用户进行黑客防御中迫切需要用到或想要用到的技术时，力求对其进行“傻瓜式”的讲解，使读者对网络防御技术形成系统了解，能够更好地防范黑客的攻击。全书共分为 11 章，主要内容包括：Windows 系统漏洞防范，木马和间谍软件的伪装与查杀，Web 攻防实战演练，QQ 与 MSN 的攻击与防御技术，电子邮件攻防实战，后门与自身防护技术，网络代理与恶意进程清除，全面提升自己的网络功能，数据备份与恢复，打好网络安全防御战等。

本书内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

图书在版编目（CIP）数据

铜墙铁壁——黑客防范技巧与工具/武新华等编著. —北京：

机械工业出版社，2009.6

（网络安全技术应用丛书）

ISBN 978-7-111-26656-3

I. 铜… II. 武… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 041019 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：丁 诚 吴鸣飞

责任编辑：吴鸣飞

责任印制：洪汉军

三河市国英印务有限公司印刷

2009 年 6 月第 1 版·第 1 次印刷

184mm×260mm·24.5 印张·604 千字

0001—4000 册

标准书号：ISBN 978-7-111-26656-3

ISBN 978-7-89451-057-0（光盘）

定价：49.00 元（含 1DVD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

销售服务热线电话：（010）68326294 68993821

购书热线电话：（010）88379639 88379641 88379643

编辑热线电话：（010）88379753 88379739

封面无防伪标均为盗版

前言

随着社会各行各业对网络技术依赖性的不断增强,人们在体验网络所带来的极大便利的同时,黑客入侵和网络安全问题也同样在困扰着网络的发展,如僵尸网络(Botnet)、网络钓鱼(Phishing)、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件、木马产业链的曝光等,更使得网络安全问题成为大家关注的焦点。

由于互联网本身的设计缺陷及其复杂性、开放性等特点,网络的安全性已成为阻碍信息化进程的重要因素,其影响已从互联网领域逐步扩大到政府、通信、金融、电力、交通等应用和建设领域。网络安全问题已引起了全世界的密切关注,黑客的恶意行为已成为全球新的公害。

或许大家都曾碰到过这样的情况,正当自己为精彩的网页着迷时,突然硬盘狂响不止,最后发现所有的程序都不能运行了;正在给网友写E-mail时,突然弹出一个对话框,上面写着“我是幽灵,我要毁了你的电脑!”;正在聊天室里与网友聊天时,突然弹出一堆对话框,无论怎么关都关不掉,最后只能无奈地重启计算机;在登录QQ时却突然提示密码错误,试遍所有可能的密码却依然不能通过,这时才发现自己的QQ密码被盗了。

因此,大家必须采取有力措施加强网络的自身安全防护性能,以有效抵抗入侵和攻击破坏。但随着攻击手段的日趋复杂,有组织、有预谋、有目的、有针对性、多样化攻击和破坏活动的频繁发生,攻击点也越来越趋于集中和精确,攻击破坏的影响面不断扩大并产生连环效应,这就势必需要构筑一种主动的安全防御,才有可能最大限度地有效应对攻击方式的变化。

写作本书的目的主要是通过介绍黑客的攻击手段和提供相应的主动防御保护措施,使读者能够循序渐进地了解黑客入侵防御的关键技术与方法,提高安全防护意识,在实际遇到黑客攻击时能够做到“胸有成竹”。希望读者能够运用本书介绍的知识去了解黑客,进而防范黑客的攻击,使自己的网络更加安全。

本书特别注重实例的讲解,针对每一种攻防手段,都结合实例来进行介绍,并紧紧围绕黑客的“攻与防”这一主线,告诉读者如何建立个人电脑的安全防护措施,使自己远离黑客攻击的困扰,确保自己电脑数据的安全。

本书通俗易懂、图文并茂,即使是电脑新手也能无障碍阅读;任务驱动式的黑客软件讲解,揭秘每一种黑客攻击的手法;最新的黑客技术盘点,让用户“先下手为强”;攻防互参的防御方法,全面确保用户的网络安全。

本书具有如下特色:

- 讲解从零起步,由浅入深,步步深入,通俗易懂,使初学者和具有一定基础的用户都能逐步提高,快速掌握黑客防范技巧与工具的使用方法。
- 理论和实例相结合,实用性强,并配以大量插图和配套光盘视频讲解,力图使读者能够融会贯通。
- 介绍大量的小技巧和小窍门,可使读者节省大量宝贵的摸索时间。
- 重点突出,内容丰富,操作步骤详细,并附有大量的操作实例,读者可以一边学习,一边在电脑上操作,做到即学即用、即用即得,快速学会操作方法。



本书在编写的过程中，得到了许多热心网友的支持，部分参考了来自网络的资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

参与本书编写的人员有武新华、刘岩、段玲华、杨平、李防、李秋菊、陈艳艳、李伟、冯世雄、孙世宁、张晓新等。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

最后，须要提醒大家的是：

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，希望读者在阅读本书后不要使用本书中所介绍的黑客技术对别人进行攻击，否则后果自负。

编 者

目 录



前言

第 1 章 Windows 系统中的漏洞	1
1.1 Windows 系统的安全隐患	2
1.1.1 Windows 操作系统中的安全隐患	2
1.1.2 Windows 操作系统中的 Bug	3
1.2 Windows 操作系统中的漏洞	5
1.2.1 Windows 系统漏洞简介	5
1.2.2 Windows 9x 中的漏洞	5
1.2.3 Windows 2000 中的漏洞	7
1.2.4 Windows XP 中的漏洞	18
1.3 黑客常用的入侵方式	21
1.4 系统安全防护对策	23
1.5 可能出现的问题与解决	26
1.6 总结与经验积累	27
第 2 章 Windows 系统漏洞防范	29
2.1 设置组策略提高系统性能	30
2.1.1 组策略简介	30
2.1.2 运行组策略	30
2.1.3 组策略中的管理模板	33
2.1.4 禁止更改【开始】菜单和任务栏	34
2.1.5 设置桌面项目	35
2.1.6 设置控制面板项目	36
2.1.7 设置系统项目	39
2.1.8 设置资源管理器	41
2.1.9 设置 IE 浏览器项目	42
2.1.10 设置系统安全	44
2.2 注册表编辑器实用防范	50
2.2.1 禁止访问和编辑注册表	50
2.2.2 设置注册表隐藏保护策略	53
2.2.3 关闭默认共享保证系统安全	55
2.2.4 预防 SYN 系统攻击	56
2.2.5 驱逐系统中自动运行的木马	57
2.2.6 设置 Windows 系统自动登录	59
2.2.7 只允许运行指定的程序	60
2.3 Windows 系统的密码保护	61

2.3.1 设置 Windows XP 的登录密码	61
2.3.2 设置电源管理密码	62
2.3.3 设置与破解屏幕保护密码	63
2.4 Windows 系统的安全设置	68
2.4.1 充分利用 Windows XP 系统的防火墙	68
2.4.2 对 Windows 系统实施网络初始化	69
2.4.3 在 IE 中设置隐私保护	70
2.4.4 利用加密文件系统加密	71
2.4.5 屏蔽不需要的系统组件	72
2.4.6 锁定计算机	73
2.5 可能出现的问题与解决	74
2.6 总结与经验积累	74
第 3 章 木马和间谍软件的伪装与查杀	75
3.1 火眼金睛识别木马	76
3.1.1 木马简介	76
3.1.2 木马的常用入侵手法曝光	79
3.1.3 木马的伪装手段曝光	80
3.1.4 识别出机器中的木马	81
3.1.5 防范木马的入侵	82
3.2 使用木马清除软件清除木马	83
3.2.1 使用“超级兔子”清除木马	83
3.2.2 使用 Trojan Remover 清除木马	91
3.2.3 使用“木马克星”清除木马	93
3.2.4 使用 360 安全卫士维护系统安全	96
3.2.5 在【Windows 进程管理器】中管理进程	100
3.3 自动安装“后门程序”的间谍软件	103
3.3.1 间谍软件简介	103
3.3.2 常见的间谍软件活动及其特点	103
3.3.3 如何拒绝潜藏的间谍软件	104
3.3.4 用 SpyBot 揪出隐藏的“间谍”	105
3.3.5 间谍广告的杀手 Ad-Aware	108
3.3.6 学会对潜藏的“间谍”说“不”	112
3.4 来自微软的反间谍专家	115
3.4.1 初识反间谍软件 Microsoft Windows Defender	116
3.4.2 手动扫描查杀间谍软件	118
3.4.3 设置定时自动扫描	120
3.4.4 开启对间谍软件的实时监控	120
3.4.5 附带的特色安全工具	121
3.5 可能出现的问题与解决	122

3.6 总结与经验积累	122
第4章 Web 攻防实战演练	125
4.1 恶意代码简介	126
4.1.1 恶意代码的特征	126
4.1.2 非过滤性病毒	126
4.1.3 恶意代码的传播方式	127
4.2 修改注册表防范恶意代码	128
4.2.1 自动弹出网页和对话框	129
4.2.2 浏览网页时被禁用了注册表	130
4.2.3 禁用 IE 查看源文件	132
4.2.4 强行篡改标题栏与默认首页地址的解决方法	132
4.3 Web 攻击与防范技术	133
4.3.1 IE 炸弹简介	133
4.3.2 防范与补救网页炸弹	135
4.3.3 ASP 脚本攻击与防御	136
4.3.4 Script 跨站攻击与防御	137
4.3.5 浏览器网址泄密的预防	138
4.3.6 清除网络实名	140
4.3.7 屏蔽多种广告	140
4.4 可能出现的问题与解决	142
4.5 总结与经验积累	143
第5章 QQ 与 MSN 的攻击与防御技术	145
5.1 常见的 QQ 攻击技术曝光	146
5.1.1 QQ 被攻击的方式曝光	146
5.1.2 使用“QQ 登录号码修改专家”查看聊天记录曝光	148
5.1.3 使用“QQ 掠夺者”盗取密码曝光	152
5.1.4 使用“QQ 机器人”盗取密码曝光	153
5.1.5 使用扫号软件获取 QQ 密码曝光	154
5.2 QQ 信息炸弹与病毒攻击曝光	155
5.2.1 用 QQ 狙击手 IpSniper 进行信息轰炸曝光	155
5.2.2 在对话模式中发送消息炸弹的常用工具曝光	160
5.2.3 向指定的 IP 地址和端口号发送信息炸弹曝光	162
5.3 保护好自己的 QQ	163
5.3.1 设置 QQ 密码保护	163
5.3.2 使用 QQ 的自带防御功能	167
5.3.3 抵御 QQ 信息炸弹	167
5.3.4 预防“QQ 枪手”盗取密码	169
5.3.5 预防并不友好的“好友号好好盗”	170
5.3.6 预防远程控制的“QQ 远控精灵”	171

5.3.7 预防“QQ 密码保护”骗子	173
5.4 MSN 的攻击和防御	174
5.4.1 MSN Messenger Hack 盗号的防范	174
5.4.2 对使用 MessenPass 查看本地密码的防范	175
5.5 可能出现的问题与解决	176
5.6 总结与经验积累	176
第 6 章 电子邮件攻防实战	179
6.1 WebMail 邮件攻防实战	180
6.1.1 来自邮件地址的欺骗	180
6.1.2 WebMail 邮箱探测的防范	180
6.1.3 邮箱密码的恢复	181
6.1.4 恶性 HTML 邮件的防范	183
6.1.5 Cookie 会话攻击的防范	186
6.2 揭秘 POP3 邮箱密码探测	187
6.2.1 黑雨——POP3 邮箱密码探测器	187
6.2.2 针对 POP3 邮箱的“流光”	188
6.3 常见 E-mail 攻击手段与防范	191
6.3.1 邮件木马	191
6.3.2 邮箱炸弹	194
6.3.3 其他方式的邮箱轰炸	196
6.3.4 邮箱炸弹的防范	197
6.3.5 设置邮箱的反垃圾功能	200
6.4 全面防范邮件病毒	201
6.4.1 邮件病毒定义及特征	201
6.4.2 邮件病毒的识别	202
6.4.3 邮件病毒的防范	203
6.5 邮件收发软件的漏洞攻防	205
6.5.1 用 Outlook Express 使联系人地址暴露	205
6.5.2 Foxmail 的账户口令封锁	207
6.5.3 清除发送邮件时留下的痕迹	209
6.6 可能出现的问题与解决	210
6.7 总结与经验积累	210
第 7 章 后门与自身防护技术	213
7.1 后门技术的实际应用	214
7.1.1 手工克隆账号技术曝光	214
7.1.2 程序克隆账号技术曝光	218
7.1.3 制造 Unicode 漏洞后门曝光	219
7.1.4 制造系统服务漏洞曝光	221
7.1.5 SQL 后门曝光	224

7.2 清除登录服务器的日志信息	225
7.2.1 手工清除服务器日志	225
7.2.2 使用批处理清除远程主机日志	226
7.2.3 通过工具清除事件日志	227
7.2.4 清除 WWW 和 FTP 日志	227
7.3 清除日志工具 elsave 和 CleanIISLog	228
7.3.1 日志清除工具 elsave 的使用	229
7.3.2 日志清除工具 CleanIISLog 的使用	230
7.4 网络防火墙技术	230
7.4.1 全面剖析 Windows XP 防火墙	230
7.4.2 功能强大的网络安全特警	233
7.4.3 黑客程序的克星——Anti Trojan Elite	242
7.5 可能出现的问题与解决	247
7.6 总结与经验积累	247
第 8 章 网络代理与恶意进程清除	249
8.1 跳板与代理服务器	250
8.1.1 代理服务器简介	250
8.1.2 跳板简介	252
8.1.3 代理服务器的设置	252
8.1.4 制作自己的一级跳板	254
8.2 代理工具的使用	255
8.2.1 代理软件 CCProxy 中的漏洞曝光	256
8.2.2 代理猎手的使用技巧	259
8.2.3 代理跳板建立全攻略	264
8.2.4 利用 SocksCap32 设置动态代理	266
8.2.5 用 MultiProxy 自动设置代理	268
8.3 恶意进程的追踪与清除	271
8.3.1 理解进程与线程	271
8.3.2 查看、关闭和重建进程	272
8.3.3 管理隐藏进程和远程进程	274
8.3.4 杀死自己机器中的病毒进程	277
8.4 可能出现的问题与解决	278
8.5 总结与经验积累	278
第 9 章 全面提升自己的网络功能	279
9.1 提升自己的网页下载权限	280
9.1.1 顺利下载被加密的网页	280
9.1.2 获得右键使用权限	283
9.1.3 突破禁用“复制/保存”功能限制	284
9.1.4 查看被加密的网页源码	285

9.1.5 有效预防网页被破解	287
9.2 使自己下载文件的权利更大	291
9.2.1 实现.swf 文件顺利下载	292
9.2.2 利用“网络骆驼”突破下载限制	293
9.2.3 顺利下载被保护的图片	294
9.2.4 顺利下载有限制的影音文件	297
9.3 给喜欢限制的网管泼点“凉水”	301
9.3.1 用 SyGate 突破封锁上网	301
9.3.2 手工实现网吧限制的突破	303
9.3.3 在网吧中一样可以实现下载	304
9.3.4 用导入注册表法解除网吧限制	305
9.4 可能出现的问题与解决	306
9.5 总结与经验积累	306
第10章 数据备份与恢复	307
10.1 数据备份	308
10.1.1 数据备份简介	308
10.1.2 实现数据备份操作	312
10.2 使用和维护硬盘数据恢复	317
10.2.1 数据恢复简介	317
10.2.2 造成数据丢失的原因	317
10.2.3 使用和维护硬盘的注意事项	318
10.2.4 数据恢复工具 Easy Recovery 和 Final Data	319
10.3 备份与恢复操作系统	325
10.3.1 系统自带的还原功能	325
10.3.2 用 Ghost 实现系统备份还原	327
10.3.3 用 Drive Image 备份/还原操作系统	330
10.4 备份与恢复 Windows Vista 操作系统	333
10.4.1 Windows Vista 自带的备份/还原功能	333
10.4.2 用安装文件备份恢复 Windows Vista 系统	336
10.4.3 用 Ghost10 实现系统备份还原	338
10.5 备份与还原其他资料	338
10.5.1 备份还原驱动程序	338
10.5.2 备份还原注册表	340
10.5.3 备份还原病毒库	341
10.5.4 备份还原收藏夹	342
10.5.5 备份还原电子邮件	344
10.6 可能出现的问题与解决	346
10.7 总结与经验积累	347

第 11 章 打好网络安全防御战	349
11.1 建立系统漏洞防御体系	350
11.1.1 检测系统是否存在可疑漏洞	350
11.1.2 修补系统漏洞的方法	352
11.1.3 监视系统的操作进程	358
11.1.4 抵抗漏洞的防御策略	360
11.1.5 防火墙安装应用实例	360
11.2 金山毒霸 2008 杀毒软件使用详解	366
11.2.1 金山毒霸 2008 的杀毒配置	366
11.2.2 用金山毒霸 2008 进行杀毒	367
11.3 东方卫士杀毒软件使用详解	369
11.3.1 东方卫士的杀毒配置	369
11.3.2 用东方卫士进行杀毒	370
11.4 江民杀毒软件 KV2008 使用详解	371
11.4.1 江民杀毒软件 KV2008 的杀毒配置	371
11.4.2 用江民杀毒软件 KV2008 进行杀毒	372
11.5 流氓软件清除详解	374
11.5.1 Wopti 流氓软件清除大师的使用	374
11.5.2 恶意软件清理助手	375
11.6 可能出现的问题与解决	376
11.7 总结与经验积累	377

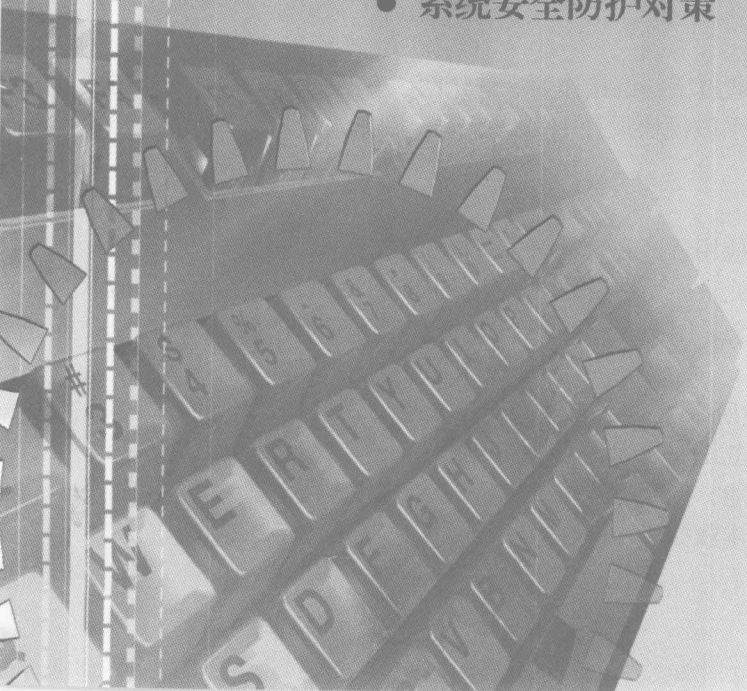
第1章

Windows 系统中的漏洞

本章精粹

重点提示

- Windows 系统的安全隐患
- Windows 操作系统中的漏洞
- 黑客常用的人侵方式
- 系统安全防护对策



Windows 操作系统是目前应用最广泛的操作平台,随着它的更新换代,其系统安全性也逐渐提高,但安全漏洞是难以彻底根除的,黑客常常利用这些漏洞对计算机实施攻击。所谓“知己知彼,百战不殆”,要想全面防止黑客的入侵,首先需要了解 Windows 操作系统中存在的一些安全漏洞和黑客攻击这些漏洞的常用方法,并掌握一些基本的安全防护策略。

1.1 Windows 系统的安全隐患

操作系统是硬件、网络与用户的一个接口。不管用户在上面使用什么应用程序或享受怎样的服务,操作系统一定是必不可少的。随着互联网的普及,网络用户的逐渐增多,由此带来的安全问题也威胁着计算机的安全,而 Windows 操作系统本身具有的漏洞,常常为黑客们的入侵行为提供了便利之门。

1.1.1 Windows 操作系统中的安全隐患

在 Windows 操作系统中,主要存在下列安全隐患。

1. 代码庞大复杂,代码重用的现象比较严重

通常情况下,程序中的 Bug 和程序的大小是成正比的。但由于 Windows 操作系统的代码量非常庞大,难免存在一些错误,而且新版本的操作系统在继承原版本重要核心代码的同时,不可避免地又继承了其原代码中存在的 Bug。

2. 盲目追求易用性和兼容性

Windows 操作系统为了增强其功能,过多地支持一些程序,默认支持的程序越多,就越容易给黑客以可乘之机,并造成系统中出现关联、兼容性等一些出乎意料的问题。

3. 无法辨别“/”和“\”

在 Windows 操作系统下一般使用“\”表示目录,但使用“/”系统也可接受,这就有可能导致在编写 ASP、PHP 以及在编写 Web 服务器之类的程序时,混用“/”和“\”而对 Web 上级目录的越权访问。

4. 设备文件名问题

Windows 操作系统的很多设备可以通过字符链接作为文件访问。有些程序在编写时,往往在防止对任意驱动器进行访问的控制手段模块设计上考虑不周。例如,使用“\D:”这样的方式即可访问 D 盘。

5. 注册表庞大而复杂

Windows 操作系统注册表中包含了应用程序和计算机系统的配置、系统和应用程序的初始化信息、应用程序和文档文件的关联关系、硬件设备的说明、状态和属性以及各种状态信息和数据等。由于注册表过于庞大和复杂,因此 Windows 操作系统很容易出现漏洞。

6. 系统的默认设置

Windows XP 系统为了提高易用性所采用的许多默认设置,也为用户增添了更多的风险。例如,为了让网络上的用户只需点击几下鼠标就可以实现文件共享,Windows XP 系统加入了一种称为“简单文件共享”的功能,但同时也打开了许多 NetBIOS 漏洞。

关闭简单文件共享功能的具体操作步骤如下:

步骤1 双击【我的电脑】图标，即可打开【我的电脑】窗口。在其中选择【工具】→【文件夹选项】菜单项，即可打开【文件夹选项】对话框，如图 1-1 所示。

步骤2 选择【查看】选项卡，在【高级设置】选项区中取消勾选【使用简单文件共享（推荐）】复选框，如图 1-2 所示。

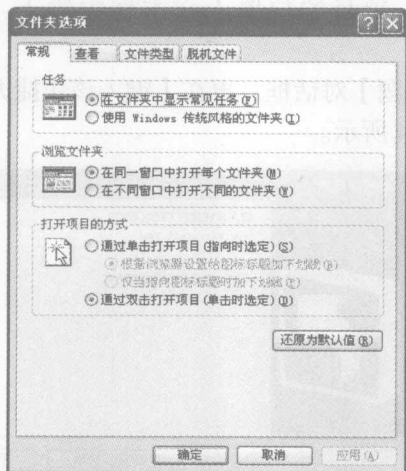


图 1-1 【文件夹选项】对话框

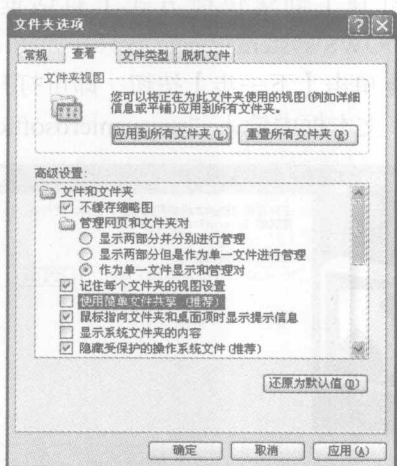


图 1-2 取消【使用简单文件共享（推荐）】复选框

7. Guest 账户

Guest 账户即来宾账户，它可以访问计算机，但会受到一定的限制。不幸地是，Guest 也为黑客入侵打开了方便之门。如果不需要用到 Guest 账户，最好禁用它。

8. Administrator 账户

Windows NT 系统有一个内建的系统管理员账号 Administrator。这个账号对整个系统拥有最高级别的控制权。在 Windows XP 系统中，这个账号被隐藏了起来，而且该账号密码是在安装操作系统时输入的。可能很多人并没有意识到这一点，因此并没有给 Administrator 账号设置密码。在这种情况下，只要有人通过网络或直接接触到用户的电脑，该用户的系统和数据就危险了。因此，如果系统中该账号密码为空，最好给这个账号设置一个密码。

9. WSH

WSH 对象非常强大，它的系统脚本引擎是默认安装的，在 IE、Office 等软件中被广泛支持，IE、Office 中的许多漏洞都与之有关。

10. 系统权限分配繁冗

Windows 2000/XP 系统中几乎每一个对象、注册表项、设备等都可以设置权限，这么庞大的访问控制列表，用户自然无法一一审核，因此，其中的很多都可以被用来作为后门。

11. 多余的服务

为了方便用户，Windows 操作系统还默认启动了许多不一定要用到的服务，同时也打开了入侵系统的后门。

1.1.2 Windows 操作系统中的 Bug

通常情况下，Windows 操作系统中的小 Bug 并不会给系统带来危害，但某些 Bug 很可

可能会被黑客利用，从而危及系统的安全。下面简单介绍 Windows 操作系统中的 Bug，以引起用户的注意。

具体的操作步骤如下：

步骤1 在桌面上单击鼠标右键，在弹出的快捷菜单中选择【新建】→【快捷方式】菜单项，即可打开【创建快捷方式】对话框，在【请键入项目的位置】文本框中输入“C:\WINDOWS\system32\calc.exe”，如图 1-3 所示。

步骤2 单击【下一步】按钮，即可打开【选择程序标题】对话框，再在【键入该快捷方式的名称】文本框中输入“www.microsoft.com”，如图 1-4 所示。

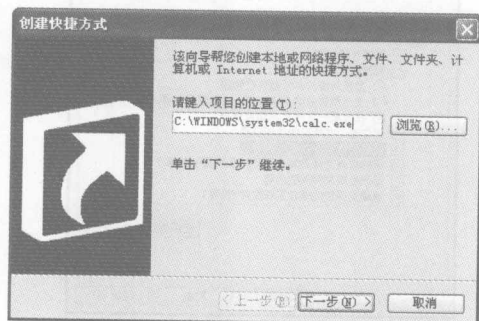


图 1-3 【创建快捷方式】对话框

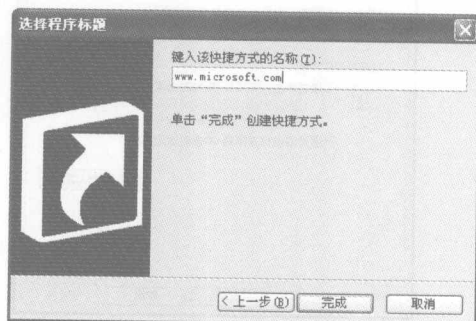


图 1-4 【选择程序标题】对话框

步骤3 单击【完成】按钮，即可完成创建。此时，桌面上将出现一个快捷方式图标。

步骤4 在 IE 浏览器地址栏中输入“www.microsoft.com”之后，即可看到此时网页并没有跳转到 Microsoft 主页中，而是打开了系统自带的计算器，如图 1-5 所示。

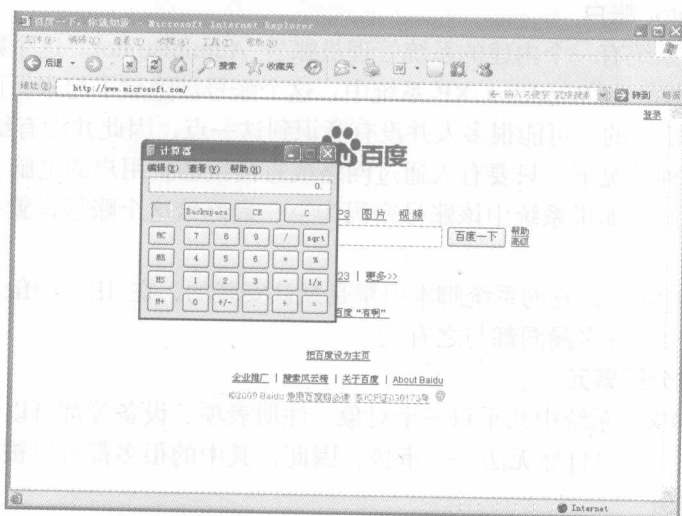


图 1-5 打开系统自带的计算器

如果 IE 浏览器没有“http: //”自动补充功能，则可启动快捷方式所指向的可执行文件。虽然微软公司已经声明该 Bug 并非安全隐患，只是 Windows 操作系统和 IE 浏览器的功能特性，类似的操作完全属于合理行为。但该 Bug 还是很容易被攻击者利用，以执行一些特

殊代码，而且不会受到 Windows 系统本身的阻挠。

1.2 Windows 操作系统中的漏洞

由于硬件原因和各种主客观因素的影响，使 Windows 操作系统中存在了一些漏洞。这些漏洞如果被别有用心的人利用，则会给用户的系统安全带来一定危险。

1.2.1 Windows 系统漏洞简介

漏洞是硬件、软件、协议的具体实现，或系统安全策略上存在的缺陷，可以使攻击者在未授权的情况下访问或破坏系统。漏洞影响到的范围非常大，包括系统本身及其支撑软件、网络客户和服务端软件、网络路由器和安全防火墙等。换言之，在不同的软、硬件设备中都可能存在安全漏洞，在不同种类的软硬件设备之间，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都存在不同的安全漏洞。

Windows 系统漏洞是特指 Windows 操作系统在逻辑设计上的缺陷，或在编写时产生的错误，这个缺陷或错误可以被不法者或电脑黑客利用，通过植入木马、病毒等方式来攻击或控制整个电脑，从而窃取电脑中的重要资料和信息，甚至破坏系统。

Windows 系统漏洞问题是与时间紧密相关的。一个 Windows 系统从发布的那一天起，随着用户的深入使用，系统中存在的漏洞将会被不断暴露出来，这些早先被发现的漏洞也会不断被系统供应商（微软公司）发布的补丁软件修补，或在以后发布的新版系统中得以纠正。而在新版系统纠正了旧版本中漏洞的同时，也会引入一些新的漏洞和错误。例如，目前比较流行的是 ani 鼠标漏洞，即是由于利用了 Windows 系统对鼠标图标处理的缺陷，木马作者制造畸形图标文件从而溢出，木马就可以在用户毫不知情的情况下执行恶意代码。

因此，随着时间的推移，旧的系统漏洞将会不断消失，新的系统漏洞也会不断出现，系统漏洞问题也会长期存在。

1.2.2 Windows 9x 中的漏洞

Windows 9x 操作系统中存在着大量的漏洞，其中有些比较典型，对今天的学习和应用仍然有相当大的参考和借鉴意义。

1. IGMP 漏洞

漏洞描述：IGMP（Internet Group Management Protocol，互联网组管理协议）漏洞是一个较有名且危险的系统漏洞，可使用户计算机中断网络连接或出现蓝屏和死机。

解释：目前有很多可发动 IGMP 攻击的工具，如 Winnuke、Sping 和 Tardrop 等。通过这些工具可向某个 IP 地址的 100 端口，不断发送大量的 IGMP 数据包，当被攻击的计算机收到数据包后，无法对数据进行处理，从而导致 TCP/IP 崩溃，引起系统中断网络连接或出现蓝屏现象，此时重启系统才可解决该问题。此外，如果攻击者进行端口监听，还可对其他端口进行攻击。

对策：

1) 下载相关的补丁程序，网址如下。

Windows 98 第 1 版：<http://www.virusview.net/download/patch/oob/up98igmp.zip>