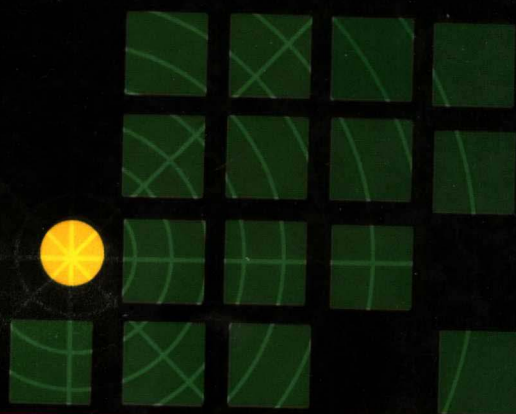




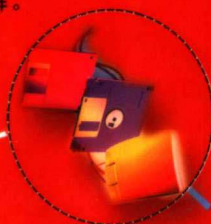
中国电脑教育报
CCID CHINA COMPUTER EDUCATION

黑客秘技万事通



罗振候 杨海 等编著

本书详细介绍了黑客的由来、黑客的攻击手段及相应的防范措施，并且对个人电脑的漏洞和网络安全知识，以及相应的反黑防毒应用作了较为详细的介绍，使读者能够对如何保护自己的电脑不受外界的危害有一个较为全面的了解。



上海科学普及出版社

黑客秘技万事通

罗振候 杨海 等 编著

上海科学普及出版社

图书在版编目 (CIP) 数据

黑客秘技万事通 / 罗振候等编著. —上海: 上海科学普及出版社, 2005. 11

ISBN 7-5427-2908-X

I. 黑… II. 罗… 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 (2005) 第 099882 号

策划编辑 胡名正

责任编辑 徐丽萍

黑客秘技万事通

罗振候 杨海 等编著

上海科学普及出版社出版发行

(上海中山北路 832 号 邮政编码 200070)

<http://www.pspsh.com>

各地新华书店经销 北京市燕山印刷厂印刷

开本 787×1092 1/16 印张 21.5 字数 512000

2005 年 11 月第 1 版 2005 年 11 月第 1 次印刷

印数 1—7100

ISBN 7-5427-2908-X/ TP · 650

定价: 29.50 元

本书如有缺页、错装或损坏等严重质量问题

请向出版社联系调换

内 容 提 要

本书由浅入深地介绍了黑客的由来、黑客的攻击手段及相应的防范措施，并且对个人电脑的漏洞和网络安全知识，以及相应的反黑防毒应用作了较为详细的介绍，使读者能够对如何保护自己的电脑不受外界的伤害有一个较为全面的了解。同时，本书还列举了各种病毒和木马的攻击与防范实例，指导读者针对各种不同的情况，使用正确的方法来解决具体问题，使自己的电脑能够安全地工作。另外，本书还给出了各种不同的计算机端口和网络命令的高级运用，使读者阅读本书后能对自己的电脑及网络构架有一个深入的了解，能够防范各种常见的黑客攻击，成为一个反黑防毒的高手。

本书内容新颖、详实，操作步骤详细明了，思路清晰，技巧丰富，并穿插有相应的提示和专业基础知识，使读者能真正做到理论与实践相结合。

本书适合不同水平层次的电脑爱好者，对一般的用户来说是一本较好的指导书籍，对专业计算机人士来说，也是一本很有参考价值的工具类书籍。



前言



在黑客日益猖獗的今天，越来越多的电脑用户遭到黑客的威胁和侵害，但是黑客是通过何种途径入侵自己的电脑，自己的电脑又存在哪些不安全的因素呢？很多电脑用户对这方面的知识还是很缺乏。而且现在各种病毒和木马泛滥，每周都会有新的病毒出现，用户如何发现自己的电脑是否受到了病毒或者木马的侵袭，又该如何清除这些病毒和木马呢？也许大多数电脑用户对此还没有很好的办法。

针对上述一系列问题，我们参阅了大量的相关文献和资料，并总结了各位电脑高手的宝贵经验，编写了《黑客秘技万事通》一书。书中对黑客的攻击手段、各种电脑系统存在的漏洞和各种病毒、木马的防范进行了详尽的介绍，并使读者能在较短的时间内掌握注册表中关于电脑和网络安全方面的基础知识。同时本书还列举了各种常见的攻击实例，使读者能依照本书自己解决在使用电脑时所遇到的各种常见的黑客问题。另外，读者通过对本书中有关网络安全章节内容的学习，能够对如何构建一个较为安全的网络有比较全面的了解，并使自己的电脑能够工作在相对安全的环境中。本书有如下几个特点：

■ 内容详实

本书精心收录了日常使用电脑时会遇到的各种病毒或者木马攻击实例，并且对每一个实例都给出具体的可行的解决办法，使读者能够根据本书的指导独立地解决在日常使用电脑时所遇到的各种常见黑客问题。

■ 内容新颖

本书挑选的例子多以最新或者最常见的病毒和木马攻击为主，能够满足绝大部分读者的需要。

■ 分类详细，便于查找

本书将各种黑客攻击针对不同的对象进行了分类，有专门独立的 MSN 和 QQ 章节、电子邮件章节、网络游戏章节、密码章节等，便于用户针对具体的情况进行查找。

■ 语言通俗易懂

本书的文字叙述力求简洁明了，通俗易懂，并在各个操作步骤中配有相关插图与提示栏，使读者无师自通。

全书共分为 14 章：第 1 章主要介绍黑客的由来及其特点；第 2 章主要介绍网络安全的基础知识；第 3 章到第 5 章则分别介绍黑客的入侵手段及防范措施、各种操作系统的漏洞；从第 6 章开始则以不同的章节分类介绍各种黑客或者病毒、木马攻击的实例及相应的防范措施；第 14 章介绍几种常见防火墙软件的使用。

上海振业电子科技有限公司组织本书的编写。本书主要由罗振候、杨海编写，杨万里高级工程师主审，参加本书编写的还有李骥、汪浩栋等人，在此一并感谢。

由于编者水平有限，又加上时间仓促，错误与不足之处在所难免，如读者在阅读过程中有什么意见或建议，请与我们联系，E-mail 发至 heroyh@sina.com.cn。

编者

2005 年 8 月

目 录

第1章 当今黑客与网络安全	1	3. TCP/IP 协议的特点	17
1.1 认知黑客	1	4. TCP/IP 的层次结构	18
1.1.1 黑客定义及其基本态度	1	5. TCP/IP 的重要协议	18
1.1.2 黑客的基本技术	2	2.2.3 UDP 协议	18
1.2 国内黑客现状	3	1. UDP 协议简介	19
1.2.1 网络系统运行的安全问题	4	2. UDP 和 TCP 协议的区别	19
1.2.2 互联网信息发布和管理中存在的问题	4	2.2.4 Internet 服务	19
1.2.3 基础信息产业严重依靠国外带来的安全问题	4	2.3 常见网络攻击	20
1.2.4 全社会的信息安全意识淡薄	4	2.3.1 网络攻击的步骤	20
1.3 面对网络安全的未来	4	1. 隐藏自己的位置	20
1.3.1 加快信息安全产业的发展	5	2. 寻找目标主机并分析目标主机	20
1.3.2 掌握安全防护知识和技术	5	3. 获取账号和密码, 登录主机	20
1.3.3 本书的目的	5	4. 使用后门, 获得控制权	20
第2章 网络基础及网络安全知识	6	5. 窃取网络资源和特权	21
2.1 基本概念	6	2.3.2 网络攻击的原理和手法	21
2.1.1 网络定义	6	1. 口令入侵	21
2.1.2 网络结构	7	2. 放置特洛伊木马程序	22
1. 物理层	7	3. WWW 的欺骗技术	22
2. 数据链路层 (DLL)	8	4. 电子邮件攻击	22
3. 网络层	8	5. 通过一个节点来攻击其他节点	23
4. 传输层	8	6. 网络监听	23
5. 会话层	8	7. 利用黑客软件攻击	23
6. 表示层	9	8. 安全漏洞攻击	23
7. 应用层	9	9. 端口扫描攻击	24
2.1.3 Internet 地址	9	2.3.3 常见的攻击工具	24
1. IP 地址的分类	10	1. DoS 攻击工具	24
2. IP 地址的识别	11	2. 木马程序	24
2.1.4 网络互联设备	11	2.3.4 相应对策	24
1. 中继器	11	1. 提高安全意识	24
2. 网桥	12	2. 采用防毒、防黑等防火墙机制	25
3. 路由器	12	3. 设置代理服务器, 隐藏自己的 IP 地址	25
4. 网关	12	4. 数据备份	25
5. 集线器	13	2.4 计算机网络的安全和管理	25
2.1.5 域名与域名系统	13	2.4.1 计算机网络安全管理的内容	26
1. 命名机制和域名解析	13	2.4.2 计算机网络安全管理的方法	26
2. 域名系统 (DNS) 及其防护	13	2.5 数据加密技术	27
2.2 网络协议	15	2.5.1 数据加密简介	27
2.2.1 网络协议的概念	16	2.5.2 各种数据加密技术介绍	27
2.2.2 TCP/IP 协议	16	1. 数据传输加密技术	28
1. TCP 协议简介	16	2. 数据存储加密技术	28
2. IP 协议简介	17	3. 数据完整性鉴别技术	28





4. 密钥管理技术	28
2.5.3 加密算法	28
1. 简单的加密方法: 换位和置换	29
2. 基于密钥的密码算法	29
3. PGP 算法	29
4. 摘要函数 (MD2、MD4 和 MD5)	30
2.5.4 数据加密物理层次	30
1. 链路加密	30
2. 节点加密	31
3. 端到端加密	31
2.5.5 数据加密的具体应用	31
1. 身份认证	31
2. 数字签名	32
3. PGP 加密系统	32
4. 加密技术在智能卡上的应用	32
2.6 硬件防火墙技术	32
2.6.1 防火墙的概念	32
1. 网络防火墙	33
2. 应用层网关防火墙	33
3. 电路层网关防火墙	33
2.6.2 防火墙配置	34
1. 分组 (或包) 过滤路由器	34
2. 双宿主网关	34
3. 主机过滤防火墙	34
4. 子网过滤防火墙	34
2.7 网络管理	34
2.7.1 OSI 网络管理结构	35
2.7.2 网络管理功能	35
2.8 常用网络命令	35
2.8.1 Net 命令	35
2.8.2 FTP 命令	37
2.8.3 DOS 下常用的相关网络命令	42
第3章 黑客入侵伎俩	44
3.1 黑客入侵的一般步骤	44
3.2 远程主机探测技术及防范	44
3.2.1 端口扫描技术及防范	44
1. 扫描器的作用	45
2. 各种扫描技术	45
3. 各种扫描工具	47
4. 如何发现扫描	47
5. 端口概念和端口分配	48
6. 查看端口	48
7. 管理端口	49
3.2.2 口令猜测及其防范	49
3.2.3 网络监听及其防范	50
3.3 黑客攻击方法及防范	51
3.3.1 拒绝服务攻击	51
1. Smurf 攻击	52
2. UDP 洪水 (UDP flood) 攻击	52
3. SYN 洪水 (SYN flood) 攻击	52
4. 泪滴 (tear drop) 攻击	53
5. Land 攻击	53
6. ping of death (死亡之 ping) 攻击	53
7. Fraggle 攻击	53
8. 电子邮件炸弹攻击	53
9. 畸形消息攻击	54
10. 分布式拒绝服务攻击 (DDoS)	54
11. 反射式分布拒绝服务攻击 (DrDoS)	54
12. DNS 分布拒绝服务攻击	54
13. 进程过载攻击	55
14. 磁盘和交换空间消耗攻击	55
15. 临时目录文件空间引起的拒绝服务	55
16. 网络的拒绝服务攻击	55
3.3.2 缓存区溢出攻击	56
3.3.3 利用程序错误攻击	57
3.3.4 欺骗类攻击	58
3.3.5 后门攻击	58
1. 口令破解后门	58
2. Rhosts ++ 后门攻击	58
3. 时间戳及校验和后门攻击	59
4. Login 后门攻击	59
5. 服务后门攻击	59
6. Cronjob 后门攻击	59
7. 库后门攻击	60
8. 文件系统后门攻击	60
9. TCP Shell 后门攻击	60
10. UDP Shell 后门攻击	60
11. ICMP Shell 后门攻击	60
12. 引导区后门攻击	61
13. Boot 块后门攻击	61
3.3.6 跳板攻击	61
1. 窃取“肉鸡”本身数据	61
2. 非法 Proxy 攻击	62
3. 平台攻击	62
4. 非法扫描、监听攻击	62
5. 端口跳转攻击	63
第4章 安全防范措施	64
4.1 个人网络安全常识	64
4.1.1 保护 IP	64
4.1.2 保护 E-Mail	64
4.1.3 保护密码	64
4.1.4 预防网络陷阱	65



4.1.5 屏蔽可疑 IP 地址	65	31. 禁用自动完成保存密码	76
4.1.6 过滤信息包	65	32. 禁止更改高级页设置	76
4.1.7 修改系统协议	65	33. 禁用连接选项	76
4.1.8 经常升级系统版本	66	34. 对拨号连接实行 “自动检测”	77
4.1.9 及时备份重要数据	66	35. 禁用缓存自动代理脚本	77
4.2 用户个人电脑的安全设置	66	36. 取消资源管理器的 文件菜单	77
4.2.1 基本防护	67	37. 禁用 Internet 连接向导	77
1. Guest 账号防护	67	38. 禁止更改代理服务器设置	77
2. 端口防护	68	39. 显示有关代理脚本下载失败的 出错信息	77
4.2.2 注册表防护	68	40. 禁用程序选项	78
1. 注册表基本操作	69	41. 禁止更改默认浏览器检查	78
2. 防止其他人非法编辑注册表	70	42. 禁止更改日历和联系人的 设置	78
3. 隐藏局域网上的服务器	70	43. 禁止更改邮件设置	78
4. 不允许用户拨号访问服务器	70	44. 禁用“重置 Web 设置”功能	79
5. 隐藏“控制面板”	70	45. 禁用高级选项	79
6. 隐藏用户登录名	71	46. 设置密码的安全要求	79
7. 禁止其他用户对桌面进行 任意设置	71	47. Windows XP 安全日志 管理技术	79
8. 抵御 BackDoor 的破坏	71	48. 禁止“显示”属性对话框中 的“Web”页	80
9. 禁止通过“文件夹选项” 显示隐藏文件	71	49. 隐藏任务栏上按右键时弹出的 菜单	80
10. 屏蔽对软盘的网络访问 功能	71	50. 禁用注册表编辑器 Regedit	80
11. 隐藏“网上邻居”图标	72	51. 禁止修改计算机账户密码	80
12. 限制用户使用指定程序	72	52. 使用注册表解锁 “光盘保镖”	80
13. 防范非法入侵 Windows XP 系统	72	53. 恢复对注册表的错误修改	81
14. 不允许他人设置屏幕保护 密码	72	4.2.3 事件日志防护	82
15. 隐藏硬盘中的分区	72	4.3 局域网安全设置	83
16. 将文件系统设置为 NTFS 格式	73	4.3.1 共享隐患	83
17. 抵御 WinNuke 黑客程序 对计算机的攻击	73	1. 蓝屏死机	83
18. 禁止用户锁定计算机	73	2. 密码漏洞	84
19. 禁止查看指定磁盘驱动器的 内容	74	3. 个人隐私	84
20. 禁止运行命令解释器和 批处理文件	74	4. 木马入侵	84
21. 禁止用户更改口令	74	4.3.2 安全设置共享文件	84
22. 禁止更改主页设置	74	4.3.3 安全设置共享打印机	85
23. 禁止更改辅助功能设置	74	4.3.4 屏蔽网络设置	85
24. 禁止更改临时文件设置	74	1. 隐藏网上邻居	86
25. 禁止更改历史记录设置	75	2. 隐藏网络图标	86
26. 禁用安全选项	75	3. 禁用网上邻居属性	86
27. 禁用内容选项	75	4. 取消网络访问权限	86
28. 禁止更改分级设置	75	4.4 SQL Server 2000 的安全配置	86
29. 禁止更改证书设置	76	4.4.1 系统设置	87
30. 禁用表单的自动完成功能	76	4.4.2 密码安全设置	87
		4.4.3 账号安全设置	87



4.4.4 数据库日志安全设置	88
4.4.5 协议加密	88
4.4.6 扩展存储过程	88
4.4.7 网络连接的 IP 限制	88
4.4.8 TCP/IP 端口安全设置	88
第 5 章 系统漏洞分析	90
5.1 操作系统漏洞	90
5.1.1 Windows 2000 漏洞及 防范措施	90
1. 登录输入法漏洞	90
2. NetBIOS 的信息泄露漏洞	91
3. 系统崩溃漏洞	93
4. IIS 服务泄露文件内容漏洞	93
5. MS SQL Server 的 SA 空密码 漏洞	94
6. Telnet 权限提升漏洞	94
7. Telnet 长用户名拒绝 服务漏洞	94
8. Telnet 拒绝服务漏洞	95
9. Telnet 多会话拒绝服务漏洞	95
10. Telnet 系统调用拒绝服务 漏洞	95
11. Telnet 会话超时导致 拒绝服务	95
12. Telnet 不同域用户账号的 访问漏洞	96
13. Lightwave ConSQLe Server 3200 telnetd 泄露信息漏洞	96
5.1.2 Windows NT 漏洞及防范措施	96
1. Windows NT 登录漏洞	97
2. Windows 网络域间信任关系 提升权限漏洞	97
3. 安全账户管理 (SAM) 数据库 被用户复制的漏洞	98
4. 紧急修复盘更新时的 SAM 漏洞	98
5. SAM 的系统特权人员漏洞	99
6. SAM 数据库和其他 Windows NT 服务器文件漏洞	99
7. 远程获得管理员特权的漏洞	99
8. 本地获取管理员特权的漏洞	100
9. 缺省 Guest 账户漏洞	100
10. 程序漏洞	100
11. 所有用户都能通过命令行方式 来接管系统共享资源的 漏洞	100
12. 无限制地尝试连接系统的 漏洞	100
13. 注册失败的次数无限制的 漏洞	100
14. 注册失败的次数限制后 解锁的漏洞	101
15. 显示最近一次注册用户名的 漏洞	101
16. 保存口令的漏洞	101
17. 口令被非 Windows NT 平台 进行同步修改的漏洞	101
18. 远程登录漏洞	102
19. Registry 权限设置漏洞	102
20. 远程访问 Registry 的漏洞	102
21. NTFS 的安全设置漏洞	102
22. 文件句柄漏洞	103
23. 缺省权限设置的漏洞	103
24. 打印操作员组成员权限 漏洞	103
25. FTP 服务漏洞	103
26. 文件移动或者复制的漏洞	103
27. 文件安全权限的漏洞	104
28. NTFS “读取”漏洞	104
29. “删除”权限漏洞	104
30. 缺省组的权限删除漏洞	104
31. 进程定期处理机制 “Bug” 漏洞	104
32. Guest 组成员资格漏洞	105
33. GUI 组最大数目漏洞	105
34. Security log 的设置漏洞	105
35. 审计文件不完全的漏洞	105
36. Security Log 集成漏洞	106
37. 屏幕保护程序 “Bug” 漏洞	106
38. 远程查询漏洞	106
39. 扫描漏洞	106
40. 端口漏洞	106
41. ping 命令漏洞	107
42. 空白口令漏洞	107
43. out-of-band 数据漏洞	107
44. IE 身份验证漏洞	108
45. HTML 超链接漏洞	108
5.1.3 Windows XP 系统漏洞及 防范措施	108
1. Windows XP 远程桌面明文 账户名传送漏洞	108
2. 账号锁定漏洞	108
3. IP 欺骗漏洞	109
4. GDI 拒绝服务漏洞	109
5. Windows XP 的 “文件和 设置转移向导” 漏洞	109
5.1.4 Linux 系统漏洞及防范措施	110
1. 内核执行拒绝服务漏洞	110



2. 内核模块 FTPFS 缓存区溢出 漏洞.....	110	5.2.3 IE5.0 ActiveX 漏洞.....	118
3. 获得本地管理员权限的 漏洞 (Linux)	111	5.3 服务器漏洞及防范措施.....	118
4. RedHat Linux IPTables 保存选项 无法恢复规则漏洞.....	111	5.3.1 Microsoft SQL Server 漏洞及 防范措施.....	118
5. RedHat Linux setserial 脚本 条件竞争漏洞.....	111	1. 函数库导致内存溢出 (buffer overrun) 漏洞.....	118
6. RedHat Linux Apache 远程列举 用户名漏洞.....	111	2. C Runtime 函数库内格式 字符串 (format string) 漏洞.....	119
7. RedHat Linux Vipw 不安全的 文件属性漏洞.....	112	3. SQL Server 2000 “扩展存储 过程”漏洞.....	119
8. RH Linux Tux HTTPD 拒绝服务漏洞.....	112	5.3.2 ASP 漏洞及防范措施.....	119
9. HP Secure OS Software for Linux 文件系统保护漏洞.....	112	1. ASP 泄露源程序漏洞.....	119
10. Linux kernel ptrace 提升权限 漏洞.....	112	2. IIS 泄露 ASP 源程序漏洞.....	120
11. Linux kernel 深层链接 拒绝服务漏洞.....	113	3. Null.htw IIS 漏洞.....	120
12. Linux Util-Linux Login Pám 权限提升漏洞.....	113	4. HTR 文件漏洞.....	120
13. Linux 2.4 Iptables MAC 地址匹配绕过漏洞.....	113	5. IIS 远程拒绝服务漏洞.....	121
14. Mandrake Linux Kernel devfs 实现漏洞.....	113	6. IIS HACK.....	121
15. Linux LPRng rhs-printfilters 远程执行命令漏洞.....	114	7. Codebrws.asp 和 Showcode.asp 漏洞.....	122
16. Linux ColdFusion CFReThrow 标签拒绝服务漏洞.....	114	8. MDAC 执行本地命令漏洞 (ASP)	122
17. SuSE Linux sdbsearch.cgi 执行 任意代码漏洞.....	114	9. ISAPI 缓冲区扩展溢出漏洞.....	122
18. SuSE Linux SuSEHelp CGI 脚本执行任意命令漏洞.....	115	10. ACCESS mdb 数据库被下载的 漏洞.....	123
19. Caldera OpenLinux DocView 特殊字符过滤漏洞.....	115	11. Code.asp 文件会泄露 ASP 代码.....	123
5.1.5 UNIX 系统漏洞及防范措施.....	115	12. File system object 组件漏洞.....	123
1. Telnetd 的缓冲区溢出漏洞.....	115	13. HTML 语句或者 JavaScript 语句的漏洞.....	123
2. Taylor UUCP 参数处理错误 漏洞.....	115	14. ASP 程序密码验证漏洞.....	123
3. UnixWare coredumps 跟随的 符号连接漏洞.....	116	5.3.3 WS_FTP Server 2.0.3 漏洞.....	124
4. UnixWare rtpm 安全漏洞.....	116	5.3.4 IPC 漏洞.....	124
5. Mtr 的安全漏洞.....	116	5.3.5 PHP 漏洞及防范措施.....	125
6. UnixWare majordomo 安全漏洞.....	117	1. PHP MyAdmin 漏洞.....	125
5.2 浏览器漏洞及防范措施.....	117	2. PHP BB 远程 SQL 查询处理 漏洞.....	125
5.2.1 IE6.0 泄露信息的漏洞.....	117	3. PHP BB \$1_statsblock 变量 远程执行代码漏洞.....	125
5.2.2 IE5.0 访问 FTP 站点时的 漏洞.....	117	4. PHProjekt 漏洞.....	125
		5. BSDi 4.2 漏洞.....	126
		6. PHP-Nuke 插入 SQL 语句 漏洞.....	126
		7. PHP-Nuke 文件泄露和上传 漏洞.....	126
		8. PHP-Nuke 的 Network Tool 漏洞.....	126
		9. PHP-Nuke 的 Cookie 漏洞.....	127
		10. PHP-Nuke 跨站脚本执行漏洞.....	127
		11. PHP-Nuke 附件漏洞.....	127





12. Unix Manual 漏洞	127
13. PHPFileExchange 漏洞	128
5.3.6 Perl 漏洞及防范措施	128
1. 用户输入漏洞	128
2. Exec()函数漏洞	129
3. System()函数漏洞	129
4. 单引号漏洞	129
5. Eval()漏洞	130
6. Setuid 脚本漏洞	130
7. 缓存区溢出漏洞	130
第6章 MSN、QQ 如何防黑杀毒	131
6.1 针对 MSN 的攻击及防范	131
6.1.1 MSN 蠕虫	131
6.1.2 “MSN 射手”	132
6.1.3 Yaha.K	132
6.1.4 Trolan.Starft	133
6.1.5 QQ 尾巴	133
6.2 针对 QQ 的攻击及防范	134
6.2.1 “QQ 神目”	134
6.2.2 “QQ 黑暗精灵”	134
6.2.3 Oicqthief	135
6.2.4 “阿 Q 盗密者” V1.1	135
6.2.5 QQSPY	136
6.2.6 “QQ 号码抢劫者”	136
6.2.7 “GOP 木马”	138
6.2.8 IPSniper	140
6.2.9 “蓝色火焰”	140
6.2.10 “潜伏猎手”	141
6.2.11 “QQ 连发器”	142
6.2.12 “QQ 杀手”	143
6.2.13 Trojan.PWS	144
6.2.14 影响 QQ 和 MSN 的病毒	145
6.2.15 FasteQQ	145
6.2.16 “QQ 之秘密潜入”	146
6.2.17 “爱情森林” (trojan.sckiss)	146
6.2.18 QQ 炸弹	146
6.2.19 骗 QQ 号的伎俩	148
6.2.20 “狐 Q”	148
6.2.21 “QQ 密码克隆专家”	149
6.2.22 防范 “QQ 千夫指”	149
6.2.23 防范 “QQ 蜗牛”	150
6.2.24 防范 “KillOICQ”	150
6.2.25 防范 “OICQ 密码终结者”	150
6.2.26 防范 “OICQhack”	150
第7章 网络游戏防黑指南	151
7.1 防范各种《传奇》木马盗号	151
7.1.1 “传奇黑眼睛”	151
7.1.2 “传奇密码窃取者”	152
7.1.3 “传奇终结者”	152

7.1.4 “传奇叛逆魔域”	152
7.1.5 “传奇精灵木马”	152
7.2 针对其他网络游戏的攻击及防范	156
7.2.1 “盗号机”专攻 中国游戏中心	156
7.2.2 “边锋杀手”	157
第8章 电子邮件的攻击和防范	159
8.1 病毒邮件查杀概述	159
8.1.1 病毒邮件的入侵形式	159
8.1.2 常见的病毒邮件	159
8.1.3 防范和处理带毒邮件	160
8.1.4 电子邮件的安全防范措施	160
8.2 Outlook Express (OE) 的漏洞及 解决手段	160
8.2.1 MIME 漏洞	161
8.2.2 Outlook 邮件附件漏洞	163
8.2.3 防止浏览信件硬盘 被格式化	163
8.2.4 VBS 病毒	164
8.2.5 Win32.Harp 病毒	166
8.2.6 OE 收发邮件的漏洞	166
8.2.7 OE 泄露联系人地址的漏洞	166
8.3 其他邮件程序的漏洞及防范	167
8.3.1 Foxmail 漏洞及防范	167
8.3.2 WEB 收信漏洞及防范	168
8.3.3 “溯雪”破解免费邮箱密码	168
8.3.4 “黑雨”破解邮箱密码	169
8.3.5 邮件炸弹	170
8.3.6 垃圾邮件	172
第9章 WEB 攻击及防范	173
9.1 ASP 脚本攻击	173
9.1.1 用户名与口令被破解	173
9.1.2 验证被绕过	173
9.1.3 .inc 文件泄露	174
9.1.4 自动备份被下载	174
9.1.5 特殊字符	174
9.1.6 数据库下载漏洞	175
9.2 My article 文章系统漏洞	176
9.2.1 My article 文章系统后台管理 口令验证失效	176
9.2.2 SQL 注入攻击	176
9.3 其他 WEB 攻击及防范	176
9.3.1 BBS XP 论坛的账号丢失	176
9.3.2 DCP Portal 系统漏洞	177
9.3.3 Discuz 论坛漏洞	177
9.3.4 惊云下载系统 SQL 漏洞	177
9.3.5 动网文章管理系统	177
9.3.6 跨站 script 攻击	178
9.3.7 脚本攻击入侵 Leadbbs	179



9.3.8 JAVA 炸弹攻击	179	12.2.2 木马的控制功能	204
第 10 章 找回丢失的密码	180	12.2.3 隐藏木马	206
10.1 密码破解概述	180	12.2.4 破解木马	207
10.2 各种系统密码	180	12.3 木马攻防	209
10.2.1 Windows 2000 密码	180	12.3.1 BO2000	209
10.2.2 Windows Me 密码	181	1. BO2K 的组成	209
10.2.3 Windows 98 密码	182	2. BO2K 的新增特性	210
10.2.4 LINUX 密码	182	3. BO2K 服务器端程序的配置	210
10.3 基于 Windows 的各种软件的密码	183	4. BO2K 客户端程序操作和命令解释	212
10.3.1 Windows 屏幕保护程序密码	183	5. 清除 BO2K 服务器端程序	216
10.3.2 WinZip 密码	183	12.3.2 冰河	216
10.3.3 WinRAR 密码	184	1. 冰河的操作	216
10.3.4 Office 系列密码	184	2. “冰河”的清除方法	218
10.3.5 ARJ 密码	185	12.3.3 广外幽灵	218
10.3.6 CMOS 密码	185	1. 广外幽灵的组成	218
10.4 各种网络服务、游戏和配置密码	187	2. 广外幽灵的操作	219
10.4.1 Foxmail 和 Outlook Express 密码	187	3. 广外幽灵的查找	219
10.4.2 Internet 选项里面的“分级审查”密码	187	4. 广外幽灵的清除	220
10.4.3 QQ 密码	189	12.3.4 黑暗天使	220
10.4.4 网络游戏密码	189	1. 黑暗天使的特点	220
10.4.5 网络配置口令	192	2. 黑暗天使的操作	221
第 11 章 网吧漏洞	194	3. 黑暗天使的防范	222
11.1 系统漏洞	194	12.3.5 聪明基因	222
11.1.1 本地硬盘漏洞	194	12.3.6 屏幕幽灵	223
11.1.2 IE 菜单漏洞	195	12.3.7 Liquid 木马	223
11.1.3 运行程序漏洞	196	12.3.8 QDe1234	224
11.1.4 资源管理器漏洞	196	12.3.9 WNC	224
11.1.5 注册表漏洞	197	12.3.10 风雪	225
11.1.6 文件操作漏洞	197	12.3.11 失恋	225
11.1.7 鼠标右键漏洞	198	12.3.12 广外女生	226
11.1.8 定制 IE 浏览器漏洞	198	12.3.13 网络神偷	227
11.1.9 IE “文件/另存为”漏洞	198	12.3.14 SubSeven	227
11.1.10 “TE 浏览器”漏洞	199	12.3.15 灰鸽子	227
11.1.11 下载漏洞	200	12.3.16 网络精灵	228
11.1.12 禁用软件漏洞	200	12.3.17 WinShell	229
11.2 网吧工具软件的漏洞	201	12.3.18 无赖小子	229
11.2.1 “美萍安全卫士”漏洞	201	12.3.19 网络魔鬼	230
11.2.2 “还原精灵”漏洞	202	12.3.20 Trojan.Zasil	230
11.2.3 “万象幻境”漏洞	202	12.3.21 PWSteal.Kaylo	231
第 12 章 木马技术大全	203	12.3.22 Trojan.Prova	231
12.1 概述木马	203	12.3.23 网络公牛	232
12.1.1 什么是木马	203	12.3.24 蓝色火焰	232
12.1.2 木马的危害及特征	203	12.3.25 BackDoor.Ducktoy	233
12.2 细说木马	204	12.3.26 BackDoor-ACH	233
12.2.1 木马的概念	204	12.3.27 国际密码	234
		12.3.28 黑洞 2001	234
		12.3.29 Funny Flash	234
		12.3.30 Webber	235
		12.3.31 Win2000 密码大盗	235



12.3.32	短文木马	235	12.4.47	Intruder	249
12.3.33	“后门”木马	236	12.4.48	IRC3	249
12.3.34	双关联木马“聪明基因”	236	12.4.49	Kaos v1.1 - 1.3	249
12.4	手工清除各种木马	237	12.4.50	Khe Sanh v2.0	249
12.4.1	冰河 v1.1& v2.2	237	12.4.51	Kuang logger	249
12.4.2	Acid Battery v1.0	238	12.4.52	Kuang Original ~ 0.34	250
12.4.3	Acid Shiver v1.0 + 1.0Mod + Imacid	238	12.4.53	Logger	250
12.4.4	Ambush	238	12.4.54	Magic Horse	250
12.4.5	AOL Trojan	238	12.4.55	Malicious	250
12.4.6	Asylum v0.1, 0.1.1, 0.1.2, 0.1.3 + Mini 1.0, 1.1	239	12.4.56	Masters Paradise	251
12.4.7	AttackFTP	239	12.4.57	Matrix v1.0 ~ 2.0	251
12.4.8	Back Construction 1.0 ~ 2.5	239	12.4.58	MBK	251
12.4.9	BackDoor v2.00 ~ v2.03	239	12.4.59	Millenium v1.0 ~ 2.0	251
12.4.10	BF Evolution v5.3.12	240	12.4.60	Mine	251
12.4.11	BioNet v0.84 ~ 0.92 + 2.21	240	12.4.61	MoSucker	252
12.4.12	Bla v1.0 ~ 5.03	240	12.4.62	Naebi v2.12 ~ 2.40	252
12.4.13	BladeRunner	240	12.4.63	NetController v1.08	252
12.4.14	Bobo v1.0 ~ 2.0	241	12.4.64	NetRaider v0.0	252
12.4.15	BrainSpy vBeta	241	12.4.65	NetSphere v1.0 ~ 1.31337	253
12.4.16	Cain and Abel v1.50 ~ 1.51	241	12.4.66	NetSpy v1.0 ~ 2.0	253
12.4.17	Canasson	241	12.4.67	NetTrojan v1.0	253
12.4.18	Chupachbra	241	12.4.68	Nirvana / VisualKiller v1.94 ~ 1.95	254
12.4.19	Coma v1.09	242	12.4.69	Phaze Zero v1.0b + 1.1	254
12.4.20	Control	242	12.4.70	Prayer v1.2 ~ 1.5	254
12.4.21	Dark Shadow	242	12.4.71	PRIORITY (Beta)	254
12.4.22	DeepThroat v1.0 ~ 3.1 + Mod (Foreplay)	242	12.4.72	Progenic Password Thief / Keylogger v1.0	254
12.4.23	Delta Source v0.5 ~ 0.7	242	12.4.73	Progenic v1.0 ~ 3.0	255
12.4.24	Der Spaeher v3	242	12.4.74	Prosiak beta - 0.70 b5	255
12.4.25	Doly v1.1 ~ v1.7 (SE)	243	12.4.75	Retrieve v1.3	255
12.4.26	Donald Dick v1.52 ~ 1.55	244	12.4.76	Revenger v1.0 ~ 1.5	255
12.4.27	Drat v1.0 ~ 3.0b	244	12.4.77	Ripper	255
12.4.28	Eclipse 2000	244	12.4.78	Satans Back Door v1.0	256
12.4.29	Eclypse v1.0	245	12.4.79	Schwindler v1.82	256
12.4.30	Executer v1	245	12.4.80	Setup Trojan (Sshare) + Mod Small Share	256
12.4.31	FakeFTP beta	245	12.4.81	ShadowPhyre v2.12.38 ~ 2.X	256
12.4.32	Forced Entry	245	12.4.82	Share All	256
12.4.33	GateCrasher v1.0 ~ 1.2	245	12.4.83	ShareQQ	257
12.4.34	Girlfriend v1.3x (Including Patch 1 and 2)	246	12.4.84	ShitHeap	257
12.4.35	Golden Retreiver v1.1b	246	12.4.85	Snid v1 - 2	257
12.4.36	Hack Tack 1.0 ~ 2000	246	12.4.86	Softwarst	257
12.4.37	Hack99 Key Logger	247	12.4.87	Spirit 2000 Beta ~ v1.2 (fixed)	257
12.4.38	Host Control v1.0	247	12.4.88	Stealth v2.0 ~ 2.16	258
12.4.39	Hvl Rat v5.30	247	12.4.89	SubSeven ~ Introduction	258
12.4.40	Iethief	247	12.4.90	Telecommando 1.54	260
12.4.41	ik97 v1.2	247	12.4.91	The Unexplained	260
12.4.42	InCommand v1.0 ~ 1.5	248	12.4.92	Thing v1.00 ~ 1.60	260
12.4.43	IndocTrination v0.1 ~ v0.11	248	12.4.93	Transmission Scout v1.1 ~ 1.2	261
12.4.44	inet v2.0 ~ 2.0n	248	12.4.94	Trinoo	261
12.4.45	Infector v1.0 ~ 1.42	248	12.4.95	Trojan Cow v1.0	261
12.4.46	iniKiller v1.2 - 3.2 Pro	248			



12.4.96	TryIt	262	13.2.33	“伪装者”	295
12.4.97	Vampire v1.0 ~ 1.2	262	13.2.34	“网络垃圾 IV”	296
12.4.98	WarTrojan v1.0 ~ 2.0	262	13.2.35	“超级密码杀手 007 变种”	297
12.4.99	Crat v1.2b	262	13.2.36	“Wininit.ini”	297
12.4.100	WebEx (v1.2, 1.3 and 1.4)	262	13.2.37	“macro.MakeLove”	298
12.4.101	WinCrash v2	263	13.2.38	Funlove”	298
12.4.102	WinCrash	263	13.2.39	“叛逃者”	299
12.4.103	Xanadu v1.1	263	13.2.40	“汉城”	300
12.4.104	Xplorer v1.20	263	13.2.41	“MSSQL” 蠕虫	300
12.4.105	Xtcp v2.0 ~ 2.1	263	13.2.42	“中国黑客”	301
12.4.106	YAT	264	13.2.43	“超级格式化”	301
第 13 章	清除各种蠕虫病毒	265	13.2.44	MP3 文件传染病毒	302
13.1	病毒杂谈	265	13.2.45	假冒 AVI 文件的病毒	302
13.1.1	认识病毒	265	13.2.46	感染 JPEG 文件的病毒	303
13.1.2	预防病毒	266	13.2.47	“IRC” 蠕虫	303
1	传染渠道	266	13.2.48	“X-WAY”	304
2	设置传染对象的属性	267	13.2.49	“振荡波”	304
13.2	各种病毒介绍及防范措施	267	13.2.50	“尼姆达”	304
13.2.1	关于宏病毒	267	13.2.51	“蓝色代码”	305
13.2.2	VBS 蠕虫生成器	268	13.2.52	CIH 病毒	305
13.2.3	“红色代码”	270	13.2.53	2003 蠕虫王	306
13.2.4	“红色结束符 II”	271	第 14 章	个人软件防火墙	307
13.2.5	“红色代码 III”	272	14.1	个人版防火墙概述	307
13.2.6	“红色代码变种”	274	14.2	Norton Internet Security 2003	307
13.2.7	“冲击波”	274	14.2.1	Norton Internet Security 2003 的安装与注册	307
13.2.8	“冲击波杀手”	275	14.2.2	Norton Internet Security 2003 的基本功能	308
13.2.9	“十四日”	276	1	安全级别设置	309
13.2.10	“蠕虫王”	276	2	隐私控制	309
13.2.11	“妖怪变种”	277	3	禁止广告	310
13.2.12	“四维”	277	4	垃圾邮件警报	311
13.2.13	“大无极”	278	5	父母控制	311
13.2.14	“大无极变种”	279	14.2.3	Norton Internet Security 2003 选项	311
13.2.15	小邮差变种 C”	279	14.3	ZoneAlarm	313
13.2.16	“老板公司变种 F”	280	14.3.1	Locked/Unlocked 功能	313
13.2.17	“神速木马”	282	14.3.2	SECURITY 级别	313
13.2.18	“费氏”	283	14.3.3	程序设置	313
13.2.19	“爱情后门”	284	14.3.4	CONFIGURE 配置面板	313
13.2.20	“雪门”	285	14.3.5	ALERTS 功能	314
13.2.21	“阿芙伦”	285	14.4	天网防火墙 (Skynet)	314
13.2.22	“求职信”	286	14.4.1	天网防火墙概述	314
13.2.23	“欢乐时光”	288	14.4.2	天网防火墙的操作	314
13.2.24	“新欢乐时光”	289	1	天网防火墙的安装	314
13.2.25	“worm.SirCam”	289	2	应用程序规则设置	315
13.2.26	“Worm.Klez”	290	3	IP 规则设置	315
13.2.27	“美丽杀手”	292	4	系统设置	316
13.2.28	“怕怕”	292	5	安全级别设置	317
13.2.29	“辛迪加”	292			
13.2.30	“Happy99”	293			
13.2.31	“MALDAL.D”	293			
13.2.32	“Sharpei/Win32.Harp”	294			

6. 其他功能.....	317
14.5 金山网镖 2003.....	318
14.5.1 概述金山网镖 2003.....	318
14.5.2 金山网镖 2003 的操作.....	318
1. 金山网镖 2003 的安装.....	318
2. 系统设置.....	318
3. 详细信息.....	318
4. 安全级别设置.....	319

5. IP 规则编辑器.....	319
6. 系统漏洞检测程序.....	319
附录 A 常见端口的攻击方法.....	320
附录 B 常见系统进程描述.....	325
B.1 基本的系统进程.....	325
B.2 附加的系统进程.....	325
B.3 其他服务进程.....	326

第1章 当今黑客与网络安全

1.1 认知黑客

提起黑客，总是那么神秘莫测。在羡慕者的眼中，他们是一些聪明绝顶、翱翔于网络空间的自由之神；在受害者眼中，他们是放荡不羁、作恶多端的害群之马，是不折不扣的电脑捣蛋分子。

那么黑客究竟是伊甸园里的那条蛇还是为人类盗来火种的普罗米修斯？是人类共同的罪犯抑或电子时代的牛仔？黑客又怎么跟电脑捣蛋分子联系在一起的呢？我们想通过本章的漫谈撩开黑客的神秘面纱。

1.1.1 黑客定义及其基本态度

“黑客”(Hacker)源于英语动词hack，意为“劈砍”，引伸为干一件非常漂亮的工作。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤其指那种手法巧妙、技术高明的恶作剧。而日本的《新黑客词典》中，把黑客定义为：“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”微软公司在其出版的1996年百科全书(光盘版)里曾对黑客下了个定义：从20世纪80年代开始，黑客这个词作为对一些人的称谓出现在计算机软件和计算机技术里。“黑客”有轻蔑的含义，通常是指喜欢通过个人计算机和拨号上网秘密地侵入另外一些计算机或计算机网络，然后查看或破坏存储在其中的数据 and 程序的人。更确切地说，黑客就是指那些通过不合法的途径进入别人的网络寻找意外满足的人。因而在如今的公众眼中，黑客又更多地与电脑捣蛋分子联系在一起，更多的情况下，他们是专搞破坏的“骇客”。

要给“黑客”下一个准确的定义是非常困难的，因为在其发展的历史中，它自身一直在进行着微妙的演变。

一般认为，黑客起源于20世纪50年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。20世纪60年代，“黑客”指独立思考、奉公守法的计算机迷。他们利用分时技术允许多个用户同时执行多道程序，扩大了计算机及网络的使用范围。20世纪70年代，黑客倡导了一场个人计算机革命，他们发明并生产了个人计算机，打破了以往计算机技术只掌握在少数人手里的局面，并提出了计算机为人们所用的观点。这一代“黑客”是电脑史上的英雄。其领头人是苹果公司的创建人史蒂夫·乔布斯。在这一时期，黑客们也发明了一些侵入计算机系统的基本技巧，如破解口令(Password cracking)、开天窗(Trapdoor)等。20世纪80年代，黑客的代表是软件设计师，包括比尔·盖茨在内的这一代黑客为个人电脑设计出了各种应用软件。与此同时，随着计算机重要性的提高，大型数据库越来越多，而信息又越来越集中在少数人手里。黑客开始为信息共享而奋斗，这时黑客开始频繁入侵各大计算机系统。如今的黑客队伍人员杂乱，既有善意的以发现计算机系统漏洞为乐趣的“电脑黑客”

(Hacker)，又有玩世不恭好恶作剧的“电脑朋克”(Cyberbunk)，还有纯粹以私利为目的、任意篡改数据、非法获取信息的“电脑攻击者”(Cracker)。如今的黑客队伍人员太多太杂，而且个个喜欢标新立异、与众不同。本书从公众理解黑客的视角出发，把黑客广义地理解为那些利用某种技术手段，善意或恶意地进入其权限以外的计算机网络空间的人。

黑客有其自身的文化，他们提倡解决问题，建设事物，信仰自由和双向的帮助，遵循着“人人为我，我为人人”的信条。要获得其他黑客的尊敬，他（她）可以做以下五种事情：

- (1) 写开放源码的软件；
- (2) 帮助测试并修改开放源码的软件；
- (3) 公布有用的信息；
- (4) 帮助维护基础设施的运转；
- (5) 为黑客文化本身服务。

黑客们虽然喜欢标新立异，与众不同，但是他们身上都有着下述一些共同的生活态度和行为特征。

崇尚自由：黑客文化首先给人的感觉就是体现出一种自由不羁的精神。黑客在电脑虚拟世界发挥着自己极致的自由，随意登录世界各地网站，完成着现实生活无法企及的冒险旅程，实现着个人生命的虚拟体验。

反叛精神：黑客骨子里对世界充满着反叛的倾向，渴望自由和平等。因特网的一个显著特点，是用户人人平等。但是，网络存在着许多禁区，有许多禁止人们随意访问的地方。黑客们认为这是有违网络特征的，他们希望建立一个没有权威、没有既定秩序的社会。所以黑客们一般都喜欢与传统、权威和集权做永不休止的斗争。

热衷挑战：黑客喜欢挑战自己的智力，编写高难度程序、破译电脑密码。而运用自己的智慧和电脑技术去突破某些著名的、防卫措施森严的站点更是一件富有刺激性、挑战性的冒险活动。这也往往是黑客价值实现的手段，“高级黑客”受人尊敬也往往是由于挑战获得成功的结果。

主张信息共享：黑客认为所有的信息都应当是免费的和公开的。黑客就是要突破对信息本身所加的限制，实现资源共享。他们认为计算机应是大众的工具，而不应是有钱人私有的。信息应该也是不受限制的，它属于每个人，拥有知识或信息是每个人的权利。

破坏心理：黑客的破坏心理源自其行为的前几个特征。黑客要在网络空间来去自由，蔑视权威，就必然要夹带着在计算机系统上的破坏举动。只有突破计算机领域防护才能随意登录各式站点；只有颠覆权威设置的程序才能反抗权威；只有摧毁网络秩序才能达到人人平等的信息共享目标。当然这和所谓的“骇客”是截然不同的，因为黑客们建设，而骇客们破坏。

1.1.2 黑客的基本技术

知己知彼，百战不殆。要想在防止黑客入侵、确保网络安全的没有硝烟的战场上处于不败之地，了解黑客攻击所必备的基本技术是必需的。

(1) 具有一定的英文水平

现在大多数资料和教程都是英文版本的，而且有关黑客的新闻也是从国外过来的，一个漏洞从发现到出现中文介绍，需要大约一个星期的时间，在这段时间内网络管理员就已经有足够的时间修补漏洞了，所以当我们看到中文介绍的时候，这个漏洞可能早已不存在了。因