

电脑



时尚与经典

9

电脑

清华天则工作室/编著

# 防黑防毒

大全

- 黑客基础
- 黑客入侵
- 黑客防范

- 认识病毒
- 检测病毒
- 病毒防范
- 防火墙

内蒙古人民出版社

73.75  
847

# 电脑时尚与经典·9

——电脑防黑防毒大全

清华天则工作室 编著

3

内蒙古人民出版社

图书在版编目(CIP)数据

电脑时尚与经典.9/清华天则工作室编著. - 呼和浩特:内蒙古人民出版社,2001.12  
ISBN 7-204-06088-1

I. 电… II. 清… III. 电子计算机-基本知识 IV. TP3

中国版本图书馆 CIP 数据核字(2001)第 090712 号

## 电 脑 时 尚 与 经 典 9

清华天则工作室 编著

\*

内蒙古人民出版社出版发行

(呼和浩特市新城西街 20 号)

新华书店发行 中国电影出版社印刷厂印刷

开本:787×1092 1/16 印张:19 字数:516 千

2002 年 3 月第一版 2002 年 3 月第一次印刷

印数:1-10000 册

ISBN 7-204-06088-1/G·1336

定价:28.00 元

# 前言

现代社会是信息化的社会,电脑和通信网络不仅被运用于军事、政治、科研、经济等重要部门,更渗透到生活的每一个角落。这些先进的科技极大地改善了人们的生活和工作方式。然而,文明的背后总会有阴影相随。先进的电脑网络带来了黑客的攻击和病毒的侵害,它们已给整个社会造成了巨大的损害,所以,保护电脑系统的安全将是至关重要的。

因此,我们编写了这本《电脑防黑防毒大全》。系统地阐述了黑客的历史性质和破坏手段及防范,病毒的种类和查杀方法,以及防火墙的设置与使用等。本书注重可读性和易操作性,尽量将晦涩难懂的专业知识作深入浅出的解析,它内容丰富、材料详实、重点突出、易学易用。不仅是信息工作人员解决安全问题的好帮手,更是一般电脑爱好者的良师益友。

本书的大概内容如下:

## 第一章 黑客基础。

本章主要讲述了黑客的基础以及防范黑客的必备知识,包括黑客的起源与发展,操作系统的安全性和网络原理基础。

## 第二章 黑客入侵。

本章主要讲述了黑客入侵的各种方法。

## 第三章 黑客防范。

本章主要讲述黑客防范的前提、方法,防范的常见问题,包括了对操作系统的设置,分析操作系统的漏洞及解决方法,黑客防范的各种各样的方法和技术,怎样才能使用户安全防范黑客的入侵,电子邮件的安全防范和木马的有关知识。

## 第四章 认识病毒。

本章讲述了病毒的常识、简介,包括病毒的概念、产生、发展特征、状况,病毒的传播及病毒的种类。

## 第五章 检测病毒。

本章讲述了病毒的发现和检测病毒的方法,包括了对软、硬件病毒的分析 and 常见的病毒类型及各种常见的病毒发现、检测和清除方法。

## 第六章 病毒防范。

主要讲述了病毒防范,包括病毒防范常见问题,网络防毒常见的问题和各种杀毒软件的设置以及使用。

## 第七章 防火墙。

这章主要讲述了防火墙常识以及各种防火墙的介绍,包括了防火墙的概念、防火墙的原理、防火墙的脆弱性以及各种防火墙的设置和使用。

# 目 录

## 第一章 黑客基础

### 第一节 认识黑客

|                              |     |
|------------------------------|-----|
| 一 什么是黑客? .....               | (1) |
| 二 什么是“快客”(Cracker)? .....    | (1) |
| 三 黑客和快客有什么区别? .....          | (1) |
| 四 黑客有什么历史? .....             | (2) |
| 五 黑客具备哪些技能? .....            | (2) |
| 六 黑客都有哪些行为准则? .....          | (3) |
| 七 黑客有自己的规则吗? .....           | (3) |
| 八 黑客的精神是什么? .....            | (4) |
| 九 黑客的目的是什么? .....            | (4) |
| 十 黑客有哪几种类型? .....            | (5) |
| 十一 如何能成为一个黑客? .....          | (6) |
| 十二 黑客是合法的吗? .....            | (7) |
| 十三 黑客行为具有哪些严重的社会危害性? .....   | (7) |
| 十四 目前的法律是否能适应打击黑客的需要? .....  | (7) |
| 十五 为什么说国际合作是打击黑客犯罪的关键? ..... | (8) |

### 第二节 网络基础知识

|                          |      |
|--------------------------|------|
| 一 什么是 Internet? .....    | (9)  |
| 二 Internet 是怎样诞生的? ..... | (9)  |
| 三 Internet 是怎样工作的? ..... | (10) |
| 四 什么是 WWW? .....         | (10) |
| 五 什么是 TCP/IP 协议? .....   | (10) |
| 六 什么是 HTTP 协议? .....     | (11) |

|                      |      |
|----------------------|------|
| 七 什么是 FTP 协议? .....  | (13) |
| 八 什么是 SMTP 协议? ..... | (14) |
| 九 什么是 IP? .....      | (15) |
| 十 什么是路由? .....       | (16) |
| 十一 什么是端口? .....      | (16) |
| 十二 什么是代理服务? .....    | (17) |

## 第二章 黑客入侵

### 第一节 口令入侵

|                        |      |
|------------------------|------|
| 一 什么是口令入侵? .....       | (18) |
| 二 口令入侵工具有哪些? .....     | (18) |
| 三 如何用口令入侵工具进行入侵? ..... | (19) |

### 第二节 特洛伊木马

|                                   |      |
|-----------------------------------|------|
| 一 什么是特洛伊木马? .....                 | (22) |
| 二 特洛伊木马的原理是什么? .....              | (22) |
| 三 特洛伊木马软件有哪些? .....               | (26) |
| 四 如何利用“冰河”进行简单攻击? .....           | (28) |
| 五 如何利用 Back Orifice 进行简单攻击? ..... | (32) |

### 第三节 监听法

|                         |      |
|-------------------------|------|
| 一 什么是监听法? .....         | (40) |
| 二 为什么以太网中可以监听? .....    | (41) |
| 三 都有什么样的监听工具? .....     | (41) |
| 四 如何使用监听工具进行网络监听? ..... | (42) |

### 第四节 隐藏技术

|                     |      |
|---------------------|------|
| 一 什么是隐藏技术? .....    | (44) |
| 二 怎样隐藏自己的 IP? ..... | (44) |

### 第五节 邮件炸弹

|                         |      |
|-------------------------|------|
| 一 什么是邮件炸弹? .....        | (45) |
| 二 都有什么样的垃圾邮件制造工具? ..... | (46) |
| 三 如何制作邮件炸弹? .....       | (47) |

### 第六节 蓝屏炸弹

|                       |      |
|-----------------------|------|
| 一 什么是蓝屏炸弹? .....      | (47) |
| 二 都有什么样的蓝屏炸弹工具? ..... | (48) |

|                             |      |
|-----------------------------|------|
| 三 黑客是怎样利用蓝屏炸弹工具进行攻击的? ..... | (48) |
|-----------------------------|------|

### 第七节 共享入侵

|                       |      |
|-----------------------|------|
| 一 什么是共享入侵? .....      | (49) |
| 二 如何利用工具进行共享入侵? ..... | (50) |

### 第八节 恶意代码入侵

|                         |      |
|-------------------------|------|
| 一 什么是恶意代码入侵? .....      | (51) |
| 二 黑客怎样利用恶意代码进行入侵? ..... | (52) |

### 第九节 Web 欺骗

|                      |      |
|----------------------|------|
| 一 什么是 Web 欺骗? .....  | (53) |
| 二 如何进行 Web 欺骗? ..... | (54) |

## 第三章 黑客防范

### 第一节 系统安装与配置

|                                                  |      |
|--------------------------------------------------|------|
| 一 怎样安全安装操作系统? .....                              | (56) |
| 二 从 Windows 98 升级到 Windows 2000 应注意哪些安全事项? ..... | (58) |
| 三 为什么 Windows 2000 比较安全? .....                   | (58) |
| 四 如何安全地设置管理员账号? .....                            | (59) |
| 五 怎样保护用户账号? .....                                | (60) |
| 六 怎样设置文件和文件夹权限以提高安全性? .....                      | (61) |
| 七 怎样设置共享文件夹或驱动器的权限以提高安全性? .....                  | (62) |
| 八 怎样利用事件审核发现安全问题? .....                          | (62) |
| 九 怎样利用磁盘数据加密,安全管理私人数据? .....                     | (64) |
| 十 怎样利用安全配置和分析,加固自己的系统? .....                     | (64) |
| 十一 怎样使用数据备份对付意外情况发生? .....                       | (66) |

### 第二节 系统漏洞及其解决

|                                        |      |
|----------------------------------------|------|
| 一 一般系统都存在哪些漏洞? .....                   | (67) |
| 二 如何解决系统的漏洞问题? .....                   | (68) |
| 三 怎样解决 Windows 2000 登录漏洞? .....        | (70) |
| 四 如何防止 NetBIOS 的信息泄漏? .....            | (72) |
| 五 怎样防止奇怪的系统崩溃? .....                   | (73) |
| 六 什么是 Telnet 的拒绝服务攻击? .....            | (73) |
| 七 如何防范 IIS 服务泄漏文件内容? .....             | (73) |
| 八 如何防范 MS SQL Server 的 SA 空密码攻击? ..... | (74) |
| 九 Windows NT 中都有哪些漏洞,如何解决? .....       | (75) |

### 第三节 注册表与安全

|                                      |      |
|--------------------------------------|------|
| 一 怎样修改注册表? .....                     | (85) |
| 二 如何备份与恢复注册表? .....                  | (85) |
| 三 怎样在登录框中隐藏用户名? .....                | (87) |
| 四 如何隐藏“文件系统”菜单? .....                | (87) |
| 五 怎样隐藏“网上邻居”? .....                  | (87) |
| 六 怎样隐藏驱动器? .....                     | (87) |
| 七 如何隐藏“关闭系统”按钮? .....                | (88) |
| 八 如何限制使用“控制面板”? .....                | (89) |
| 九 怎样拒绝远程访问软驱? .....                  | (89) |
| 十 如何拒绝远程访问光驱? .....                  | (89) |
| 十一 怎样锁定桌面? .....                     | (89) |
| 十二 如何锁定桌面背景? .....                   | (89) |
| 十三 如何禁用 Regedit 命令? .....            | (90) |
| 十四 怎样锁定“开始”菜单? .....                 | (90) |
| 十五 怎样预防 WinNuke 的破坏? .....           | (90) |
| 十六 怎样禁用“任务栏属性”功能? .....              | (90) |
| 十七 如何禁止修改显示属性? .....                 | (91) |
| 十八 怎样禁止屏幕保护使用密码? .....               | (91) |
| 十九 Windows 98 中如何限制非法用户登录? .....     | (91) |
| 二十 Windows 98 如何查看共享密码? .....        | (92) |
| 二十一 如何在关机时清除 Pagefile 文件? .....      | (94) |
| 二十二 如何限制应用程序的使用? .....               | (94) |
| 二十三 如何在 IE 中加入第五个安全区? .....          | (94) |
| 二十四 如何禁止对注册表的远程访问? .....             | (95) |
| 二十五 如何限制对注册表的匿名访问? .....             | (95) |
| 二十六 在 Windows NT 下如何审核对注册表的改变? ..... | (95) |
| 二十七 如何修复注册表的错误? .....                | (96) |

### 第四节 系统维护

|                                  |       |
|----------------------------------|-------|
| 一 Windows 2000 中如何维护系统文件? .....  | (96)  |
| 二 如何制作 Windows 2000 系统启动盘? ..... | (96)  |
| 三 如何对 LOG 文件进行管理? .....          | (97)  |
| 四 Windows 2000 如何进行入侵监测? .....   | (98)  |
| 五 如何利用 Windows 2000 的二次登录? ..... | (102) |
| 六 怎样设置 CMOS 密码? .....            | (103) |
| 七 怎样“加密”目录? .....                | (104) |
| 八 怎样加密各种办公文件? .....              | (104) |
| 九 怎样为 FoxMail 加密? .....          | (105) |
| 十 怎样对压缩文件进行加密? .....             | (105) |

## 第五节 黑客防范方法

|                              |       |
|------------------------------|-------|
| 一 怎样防范口令入侵? .....            | (105) |
| 二 怎样防范特洛伊木马? .....           | (106) |
| 三 怎样防范监听法? .....             | (107) |
| 四 怎样防范垃圾邮件和邮件炸弹? .....       | (108) |
| 五 遭受邮件炸弹袭击后应该怎么办? .....      | (109) |
| 六 怎样防范共享文件入侵? .....          | (110) |
| 七 如何防范 Windows 远程共享漏洞? ..... | (111) |
| 八 如何防范 Web 欺骗? .....         | (111) |

## 第六节 用户安全防范常见问题

|                                    |       |
|------------------------------------|-------|
| 一 怎样的口令才算安全? .....                 | (112) |
| 二 一般要注意哪些保密技巧? .....               | (113) |
| 三 如何防范 TXT 文件欺骗? .....             | (114) |
| 四 用 QQ 聊天需要注意哪些问题? .....           | (115) |
| 五 如何用软件修改 QQ 的端口设置? .....          | (116) |
| 六 IE 浏览器有哪些安全漏洞? .....             | (117) |
| 七 浏览网页需要注意哪些问题? .....              | (117) |
| 八 Web 聊天需要注意哪些问题? .....            | (118) |
| 九 什么是浏览器安全区域? .....                | (119) |
| 十 怎样给区域设置安全级别? .....               | (120) |
| 十一 怎样自定义安全级项目? .....               | (121) |
| 十二 什么是 ActiveX 插件和控件? .....        | (122) |
| 十三 如何对 ActiveX 进行安全设置? .....       | (122) |
| 十四 什么是 Cookie? .....               | (123) |
| 十五 如何对 Cookie 进行安全设置? .....        | (123) |
| 十六 什么是脚本? .....                    | (123) |
| 十七 怎样设置脚本的执行权限? .....              | (123) |
| 十八 如何对 JVM 进行安全设置? .....           | (123) |
| 十九 如何对浏览器中的“下载”选项进行安全设置? .....     | (124) |
| 二十 怎样设置浏览器中的“用户验证”? .....          | (124) |
| 二十一 如何对浏览器中的“其他”选项进行设置? .....      | (125) |
| 二十二 如何将 Web 站点分配到安全区域? .....       | (125) |
| 二十三 什么是分级审查? .....                 | (126) |
| 二十四 如何启用和设置分级审查? .....             | (126) |
| 二十五 如何指定他人永远能够或不能查看的 Web 站点? ..... | (127) |
| 二十六 如何允许他人查看受限制的内容? .....          | (127) |
| 二十七 怎样对浏览器进行高级安全设置? .....          | (128) |
| 二十八 怎样防止 IE 中 FTP 密码泄露? .....      | (129) |

## 第七节 电子邮件安全防范

- 一 订阅邮件列表需要注意哪些问题? ..... (130)
- 二 如何设置电子信箱的密码? ..... (131)
- 三 怎样给我的电子邮件加密? ..... (132)
- 四 怎样追踪垃圾邮件? ..... (135)
- 五 怎样对付垃圾邮件制造者? ..... (136)

## 第八节 木马常见问题

- 一 木马都用哪些对应端口? ..... (137)
- 二 怎样发现和清除木马? ..... (140)
- 三 怎样利用批处理程序清除木马? ..... (141)
- 四 发现木马后应该怎么清除? ..... (142)

# 第四章 认识病毒

## 第一节 病毒常识

- 一 什么是病毒? ..... (157)
- 二 病毒是怎样产生的? ..... (158)
- 三 编写病毒的目的是什么? ..... (159)
- 四 病毒怎样传播? ..... (160)
- 五 病毒有哪些感染方式? ..... (160)
- 六 病毒可以造成哪些危害? ..... (161)
- 七 病毒有哪些特征? ..... (162)
- 八 病毒有哪些类型? ..... (163)
- 九 计算机感染病毒后有哪些症状? ..... (165)
- 十 病毒怎样命名? ..... (165)
- 十一 怎样面对病毒? ..... (166)
- 十二 病毒的发展状况如何? ..... (166)

## 第二节 常见病毒简介

- 一 病毒经历了哪些历史? ..... (168)
- 二 病毒由哪些部分组成? ..... (169)
- 三 什么是引导型病毒? ..... (170)
- 四 引导型病毒如何传播? ..... (170)
- 五 什么是文件型病毒? ..... (170)
- 六 什么是宏病毒? ..... (171)
- 七 宏病毒是怎么传染的? ..... (171)

## 第五章 检测病毒

### 第一节 病毒检测方法

|                        |       |
|------------------------|-------|
| 一 如何发现病毒? .....        | (173) |
| 二 有哪些病毒检测方法? .....     | (173) |
| 三 哪些硬件故障与病毒现象类似? ..... | (175) |
| 四 哪些软件故障和病毒现象类似? ..... | (176) |

### 第二节 病毒的检测和清除

|                         |       |
|-------------------------|-------|
| 一 常见的一些病毒如何检测与清除? ..... | (177) |
| 二 如何检测和清除宏病毒? .....     | (186) |
| 三 如何检测和清除蠕虫病毒? .....    | (190) |
| 四 如何检测和清除特洛伊病毒? .....   | (214) |

## 第六章 病毒防范

### 第一节 病毒防范常见问题

|                             |       |
|-----------------------------|-------|
| 一 怎样保持计算机不染病毒? .....        | (219) |
| 二 计算机感染了病毒怎么办? .....        | (220) |
| 三 碰到可疑的目标怎么办? .....         | (220) |
| 四 怎样对付宏病毒? .....            | (220) |
| 五 发现 doc 里有病毒,怎样手工杀除? ..... | (222) |
| 六 怎样防范 Word 宏病毒? .....      | (222) |
| 七 如何判断是否感染 Word 宏病毒? .....  | (223) |
| 八 忽然遇到宏病毒发作该怎么办? .....      | (224) |
| 九 如果我不自定义宏也会感染宏病毒吗? .....   | (224) |

### 第二节 网络防毒常见问题

|                         |       |
|-------------------------|-------|
| 一 有哪些对病毒的错误认识? .....    | (224) |
| 二 有 Internet 病毒吗? ..... | (225) |
| 三 当传输文件时可能感染病毒吗? .....  | (226) |
| 四 浏览网页会中毒吗? .....       | (226) |
| 五 如何对电子邮件进行病毒防护? .....  | (226) |
| 六 如何对电子邮件系统进行保护? .....  | (227) |
| 七 使用外来磁盘时如何防范病毒? .....  | (228) |
| 八 用软盘启动机器会有什么危害? .....  | (229) |
| 九 下载软件应该注意哪些问题? .....   | (229) |

|                         |       |
|-------------------------|-------|
| 十 如何查杀压缩文件的病毒? .....    | (229) |
| 十一 如何防范病毒侵袭 BIOS? ..... | (230) |
| 十二 如何选择杀毒软件? .....      | (231) |
| 十三 如何合理搭配杀毒软件? .....    | (232) |

### 第三节 杀毒软件 McAfee VirusScan 的使用

|                                  |       |
|----------------------------------|-------|
| 一 什么是 McAfee VirusScan? .....    | (234) |
| 二 McAfee VirusScan 有哪些新功能? ..... | (234) |
| 三 如何安装 McAfee VirusScan? .....   | (235) |
| 四 如何利用 McAfee 查杀病毒? .....        | (240) |
| 五 如何利用 McAfee 实时监测病毒? .....      | (241) |
| 六 McAfee 怎样使用计划任务? .....         | (242) |
| 七 McAfee 怎样升级病毒代码库? .....        | (242) |
| 八 怎样对 McAfee 进行其他重要设置? .....     | (243) |

### 第四节 杀毒软件《金山毒霸》的使用

|                        |       |
|------------------------|-------|
| 一 什么是《金山毒霸》? .....     | (243) |
| 二 《金山毒霸》有哪些特性? .....   | (243) |
| 三 怎样安装《金山毒霸》? .....    | (244) |
| 四 怎样启动和退出《金山毒霸》? ..... | (244) |
| 五 怎样定制查毒内容? .....      | (245) |
| 六 查到病毒如何处理? .....      | (246) |
| 七 怎样定时查毒? .....        | (246) |
| 八 如何进行相关选项的设置? .....   | (247) |
| 九 怎样设置和查看日志文件? .....   | (250) |
| 十 怎样创建应急盘? .....       | (250) |
| 十一 怎样升级病毒库? .....      | (251) |

## 第七章 防火墙

### 第一节 防火墙常识

|                       |       |
|-----------------------|-------|
| 一 什么是防火墙? .....       | (252) |
| 二 防火墙的工作原理是什么? .....  | (253) |
| 三 防火墙有哪些特点? .....     | (254) |
| 四 防火墙技术有哪些种类? .....   | (254) |
| 五 为何需要防火墙? .....      | (256) |
| 六 防火墙可以防范什么? .....    | (256) |
| 七 防火墙不能防范什么? .....    | (257) |
| 八 防火墙能否防止病毒的攻击? ..... | (257) |

|                              |       |
|------------------------------|-------|
| 九 防火墙有哪些基本类型? .....          | (257) |
| 十 防火墙都有哪些实现方式? .....         | (259) |
| 十一 怎样才能穿过防火墙使用 FTP? .....    | (260) |
| 十二 怎样才能穿过防火墙使用 Telnet? ..... | (260) |
| 十三 防火墙怎样防止别人探测你的 IP? .....   | (260) |
| 十四 防火墙怎样防止蓝屏攻击? .....        | (261) |
| 十五 防火墙如何防止共享入侵? .....        | (261) |
| 十六 防火墙怎样防止冰河入侵? .....        | (261) |
| 十七 怎样看待安全记录? .....           | (261) |
| 十八 防火墙的未来发展趋势如何? .....       | (262) |
| 十九 都有哪些常见的防火墙? .....         | (262) |
| 二十 防火墙有哪些缺陷? .....           | (264) |
| 二十一 传统防火墙都有哪些不足? .....       | (265) |
| 二十二 常见的针对防火墙的攻击方法有哪些? .....  | (265) |

## 第二节 天网防火墙的使用

|                         |       |
|-------------------------|-------|
| 一 什么是天网防火墙? .....       | (267) |
| 二 天网防火墙有哪些特点? .....     | (267) |
| 三 怎样安装天网防火墙? .....      | (268) |
| 四 如何运行天网防火墙? .....      | (269) |
| 五 如何根据自身特点进行安全设置? ..... | (269) |

## 第三节 防火墙 LockDown2000 的使用

|                             |       |
|-----------------------------|-------|
| 一 什么是 LockDown2000? .....   | (275) |
| 二 LockDown2000 有哪些功能? ..... | (275) |
| 三 怎样安装 LockDown 2000? ..... | (276) |
| 四 怎样运行 LockDown 2000? ..... | (276) |
| 五 如何进行系统黑客程序的扫描? .....      | (276) |
| 六 如何设置 LockDown 2000? ..... | (278) |
| 七 怎样查看和分析各种网络记录? .....      | (279) |

# 第一章 黑客基础

## 第一节 认识黑客

### 一 什么是黑客？

当今社会,提起黑客不得不令人心惊胆战,黑客问题也是人们不得不正视的一个问题之一。在网络时代,“黑客大战”成了人们熟悉的“战争”。那么,什么是黑客,黑客是从哪里来的呢?

“Hacker”(黑客)一词来自于英语动词“Hack”,这个词在英文中有“乱砍、劈、砍”之意,它的一个引申意义是指“干了一件非常漂亮的事”。十九世纪 60 年代,电脑系统是非常昂贵的,只是存在于各大院校与科研机构的“玻璃房”中,技术人员使用一次电脑,需要很多复杂的手续,而且电脑的工作效率也不是很高。为了绕过一些限制从而最大限度地利用这些昂贵的电脑系统,最初的程序员们就写出了一些简洁高效的捷径程序,这些程序往往较原有的程序系统更完善、更简便,而这种行为便被称为 Hack。如今,黑客的普遍含义是电脑系统的非法入侵者,他们精通计算机及相关的科学,具备了良好的科学素质,经常研究开发出许多新的具有开创意义的产品或技术,他们以进入他人防范严密的计算机系统为生活的一大乐趣,并以此来评定自身的价值。

### 二 什么是“快客”(Cracker)?

有些人认为黑客与快客是同一种人,他们都是电脑有意、无意的破坏者,那么,快客又是什么?

“Cracker(快客)”在英文中有“破坏者”之意,他们做的事更多的是破解商业软件、恶意入侵别人的网站并造成损失,而且手法巧妙、技术高明。

### 三 黑客和快客有什么区别?

黑客与快客都是计算机方面的高手,他们都具有很强的技术水平、理解能力以及高超的创新技能。也就是说,快客具有黑客的本领,只不过是在行事上有些差别而已,这也是我们常常很难分清黑客与快客的原因之一。有些人认为,黑客就是在网络上非法侵入别人机器的人;也有些人认为黑客创造东西,而快客只破坏。其实,无论是黑客还是快客,名称只是一种代号而已,他们之间并无绝对的界限,我们也很难将他们区分得很清楚,他们都是非法入侵者。既是非法入侵者,再区分什么善意入侵与恶意入侵也就没有意义了,而且无论是哪一种入侵,无论是有意还是无意,都有可能造成被入侵者的损失。

## 四 黑客有什么历史?

正如前面所说的,黑客专门对计算机进行非法入侵,对计算机进行破坏;然而黑客曾经对计算机的发展起到了重要的作用,甚至,黑客曾有自己值得骄傲的时代,他们也曾代表着计算机运用的先锋,也是人们所欢迎的“技术专家”。可在当今,黑客虽是人们不得不敬佩的群体,却也成了人们所惧怕的对象,正所谓“又爱又恨”。那么黑客到底有什么辉煌的历史呢?

随着计算机的产生与发展,黑客也应运而生,并且有了属于自己的文化——黑客文化。在黑客王国里,各种各样的高技术随处可见,那么,黑客对计算机的发展到底是好是坏呢?有一种观点认为,黑客对电脑技术的革新与扩展做出了不可磨灭的贡献,他们创造出许多新颖而独特的软件,而近些年来互联网的飞速发展,也有黑客的一份功劳在其中,许多网络破绽都是由于黑客们的努力而得到解决的。

但是有些人对此观点嗤之以鼻,他们认为,黑客就是搞破坏的,就是不道德的。我们只要回顾一下黑客发展的历史,就会发现这种说法并不过分。Hacker 这个称谓在早期是令人自豪的,直到现在仍有人以被称为 Hacker(黑客)而自豪,并以洁身自好的姿态与“Cracker”(快客们)区分开来。的确,最早的 Hacker 是一种褒义词,只有那些最优秀的技术专家才能被冠以 Hacker 的称号。这可以追溯到几十年前第一台微机刚诞生的时候。那时因特网的雏形 ARPANET 也刚刚建立,当时能够使用这个网络的都是一些程序设计专家或是科学家等,是一群处于高科技最前沿的人们,而正是这些人创造了 Hacker 这个词。从某种意义上,可以把这些最早的 Hacker 视为 Internet 的创始人,正是他们开发出了强大的迄今仍在使用的 UNIX 操作系统,这就是最早的黑客。他们具有高超的技术、过人的智力以及坚韧的探索未知事物的毅力。他们对电脑技术的发展,对因特网的发展,都做出了巨大的贡献,这些黑客是值得尊敬的。

但是到了 70 年代,情况发生了变化,更多的黑客出现了,这些黑客也同样具有高超的技术,他们以侵入别人的系统为乐,随意修改别人的资料,使得黑客这个称谓逐渐变得不那么令人喜欢。同时因为大量的黑客及黑客技术的涌现,加上因特网的发展,让黑客与黑客之间的交流更容易,在因特网上也出现了专供黑客交流的 BBS,黑客逐渐形成了科技领域尤其是电脑领域的一个独特的群体。

## 五 黑客具备哪些技能?

黑客的真正实力在于对计算机的很好地运用,黑客的力量并非一句话可以概括。真正的黑客,有着很强的知识力量和丰富的经验教训,要想当一名真正黑客并不是一件容易的事,但只要肯下工夫也不见得很难。一般情况下,黑客应具有下面的基本技能:

### 1. 程序设计

当然,这是基础的 Hacking 技能。但是,如果你只是学一种语言,也不能算是一位 Hacker,最多只能算一个 Programmer,你还必须学会以独立于任何程序语言之上的概括性观念来思考程序设计上的问题。要成为一位真正的 Hacker,你必须能在几天之内将软件手册内容和你已经知道的联系起来,学会一种新的语言。你必须学会数个不同的语言,你至少还要会 LISP 或 Perl,这些语言提供你一些不同的程序设计途径,并且让你在好的方法中学习。要学好程序设计,应养成读别人的程序和写自己程序的习惯。

### 2. 会写 HTML

Hacker 文化创造出来的东西,大多在他们的活动范围外被使用着。如在工厂和办公室或大学被使用着。但 Web 是一个很大的例外,它悄悄地在改变这个世界,因此你必须学习 Web。并不只是学习使用浏览器而已,还要学会写 HTML——Web 的标签语言。如果你不知道如何设计程序,写 HTML 也能给你一些帮助。

### 3. 使用和维护 UNIX

取得黑客技巧的第一个步骤是取得一份 LINUX 或者一份免费的 BSD - UNIX, 并将它安装在自己的机器上使之顺利地运作。虽然在这个世界上除了 UNIX 之外, 还有其他的操作系统, 但是他们只提供 Binary, 你不能看到他们的程序码, 也不能修改他们。想要在 DOS、Windows 或 MacOS 开始 Hacking, 无疑就是要你绑着枷锁跳舞。除此之外, UNIX 是 Internet 上的操作系统, 当你在不懂 UNIX 的情况下学习使用 Internet 时, 你没办法成为 Internet 的黑客。因为这个原因, 现在的黑客文化还是很牢固地以 UNIX 为中心(这并不完全是正确的, 而且有些活在旧时代的黑客甚至也不喜欢, 但是 UNIX 和 Internet 之间的共生共存已经到了牢不可破的地步)。因此, 把 UNIX 装起来吧! 学习它, 让它运作起来, 让它陪你努力精进。用它向整个 Internet 喊话、看程序码、改程序。有一天你成为一位高竿的黑客, 回头往后看时会发现, 你得到的是比 Microsoft 操作系统所能提供的还要好的程序设计工具。

## 六 黑客都有哪些行为准则?

黑客们一再声称自己与“快客”的不同, 于是便对黑客的行为准则有了各种各样的注释, 但总结起来, 不外乎以下几条:

### 1. 不随便攻击个人用户及站点

虽然黑客们在找到系统漏洞并侵入时往往都会很小心, 尽量避免造成损失, 并尽量善意地提醒管理者, 但在这过程中有许多因素是未知的, 没有人能肯定最终会是什么结果, 因此一个好的黑客是不会随便攻击个人用户及站点的。

### 2. 多编写一些有用的软件

这些软件都是免费的, 但又和一般的共享软件有所不同, 因为共享软件并不公开其源代码, 而这些软件的源代码往往也是公开的。

### 3. 帮助别的黑客测试与调试软件

没有人能写出没有一点错误或是不需要改进的完美软件, 因而对软件的测试与调试是非常重要的, 测试与调试软件甚至比编写软件更耗费精力。但在黑客的世界中这算不了什么, 因为在你编写出一个软件之后, 会有许多的黑客热心地帮助你测试与调试。

### 4. 力所能及地义务做一些事

黑客们都以探索漏洞与编写程序为乐, 但在黑客的圈子中, 除了探索漏洞与编写程序外, 还有许多其他的杂事, 如维护和管理相关的黑客论坛、新闻讨论组以及邮件列表, 维持大的软件供应站, 推动 RFC 和其他技术标准等等。这些事都需要人来做, 但也许并不都是那么令人感到有趣。所以, 那些花费大量精力, 义务地为网友们整理 FAQ、写教程的黑客以及各大黑客站点的站长, 在网络上都是令人尊敬的。

### 5. 洁身自好, 不和快客混在一起

真正的黑客总是耻于与快客为伍, 他们不会随意破解商业软件并将其广泛流传, 也不会恶意侵入别人的网站并造成损失。他们的所作所为更注重对于网络安全的监督。

## 七 黑客有自己的守则吗?

黑客崇尚的是自由, 他们有组织, 但都是一些松散的、为了讨论技术而存在的组织。而所谓的黑客守则, 也不像是我们日常生活中的这样那样以各种形式制定的守则, 事实上, 这是一群最崇尚自由的人, 他们最不喜欢的就是规则, 所以并没有绝对的黑客守则。但黑客对自己的技术都很自豪, 不喜欢别人误解自己, 也不喜欢别人将黑客与快客混在一起, 因而在互联网上便流传着种种黑客们自律的“黑客守则”。黑客守则有多种版本, 比较典型的一种如下: