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

- 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

电脑时尚与经典·9

——电脑防黑防毒大全

清华天剑工作室　编著

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。

这章主要讲述了黑客的基础以及防预黑客的必备知识，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。

这章主要讲述了黑客入侵的各种方法。

第三章 黑客防范。

这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。

这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。

这章讲述了病毒的发现和检测病毒的方法，包括了对软、硬件病毒的分析和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

第二节 网络基础知识

第二章 黑客入侵

第一节 口令入侵

第二节 特洛伊木马

第三节 监听法

第四节 隐藏技术

第五节 邮件炸弹

第六节 蓝屏炸弹

第三章　黑客防范

第一节　系统安装与配置

第二节　系统漏洞及其解决

第三节 注册表与安全

第四节 系统维护

第五节　黑客防范方法

第六节　用户安全防范常见问题

第七节 电子邮件安全防范

第八节 木马常见问题

第四章 认识病毒

第一节 病毒常识

第二节 常见病毒简介

第五章　检测病毒

第一节　病毒检测方法

第二节　病毒的检测和清除

第六章　病毒防范

第一节　病毒防范常见问题

第二节　网络防毒常见问题

第三节 杀毒软件 McAfee VirusScan 的使用

第四节 杀毒软件《金山毒霸》的使用

第七章 防火墙

第一节 防火墙常识

第二节　天网防火墙的使用

第三节　防火墙 LockDown2000 的使用

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困难。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目前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 LINUIX 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 Bianry，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：