用电脑不求人系列之十五

GOTOP

# 防范黑客不求人

林东和 编著
樊小溪 改编

你知道 你的电脑
已经被 黑客入侵 了吗?
如何发现? 如何预防?

- Windows系统漏洞
- Windows系统入侵伎俩
- 防范 Windows 系统密码入侵
- 防范特洛伊木马入侵
- 防范 E-mail入侵
- 防范 Intranet入侵

人民邮电出版社
www.pptph.com.cn

用电脑不求人系列之十五

# 防范黑客不求人

林东和　编著

樊小溪　改编

人民邮电出版社

**图书在版编目(CIP)数据**

防范黑客不求人/林东和编著.-1 版.-北京：人民邮电出版社，2000.09
(用电脑不求人系列之十五)
ISBN 7-115-00000-0

I.选… II.林… III.电子计算机-硬件-基本知识 IV.TP33

中国版本图书馆 CIP 数据核字(1999)第 00000 号

用电脑不求人系列之十五

**防范黑客不求人**

◆ 编　　著　林东和
改　　编　樊小溪
责任编辑　俞　彬

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ pptph.com.cn
网址　http://www.pptph.com.cn
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销

◆ 开本:720×980　1/16
印张:19
字数:367 千字　　2001 年 1 月第 1 版
印数:6 001 - 12 000 册　　2001 年 2 月北京第 2 次印刷

著作权合同登记　图字:01 - 2000 - 3589 号
ISBN 7-115-09037-8/TP·2008

定价:32.00 元

# 内容提要

本书是一本专门探讨黑客入侵的书籍。本书通过简单图例及使用步骤说明，按部就班、循序渐进地分析出黑客入侵的伎俩，进而找出系统漏洞并加以补救。

本书第一章介绍了有关黑客的基本知识。第二章让您认识黑客及其入侵的常用伎俩。第三章介绍电脑的 IP 与 PORT 的正确概念。第四章介绍了 Windows 系统的安全漏洞。第五章介绍了 Windows 系统密码入侵的常用方法。第六章以 Subseven 为例，介绍了特洛伊木马入侵的常用方法。第七章介绍了 E-mail 入侵常用方法。第八章探讨了 Intranet 入侵常用方法，并介绍了防范内部网络入侵的对策。第九章介绍了局域网防火墙技术。第十章则总结性地介绍了黑客入侵流程。本书附录提供了黑客入侵常用姓名和 PORT 端口的定义及说明。

# 版权声明

# 出版说明

在计算机技术飞速发展的今天，为了进一步向全社会普及计算机知识，提高计算机应用人员的技术水平，使计算机在各个领域发挥更大作用，也为了促进海峡两岸计算机技术图书的交流，台湾碁峰资讯股份有限公司授权我社陆续组织出版该公司的部分计算机技术书籍。这些书基本覆盖了当前最常用的各类计算机软、硬件技术，并紧跟世界上计算机技术的飞速发展，不断有所更新。在写作特点上，这些书内容深入浅出、实用性强，在台湾地区很受读者欢迎。

在组织出版过程中，我们请有关专家在尊重原著的前提下，进行了改编，并对有关图文进行了核对和精心制作。

由于海峡两岸的计算机技术名词和术语差异较大，改编者依照有关规定和我们的习惯用法进行了统一整理。

对原书文字叙述中由于海峡两岸不同的语言习惯而造成的差异，我们的处理原则是只要不会造成读者理解上的歧义，一般没做改动，以尊重原著写作风格。另外改编时对原书的一些差错及疏漏之处做了订正。

由于本书改编和出版时间紧张，如有差错和疏漏，敬请读者指正。

人民邮电出版社

2000.9

# 商 标 声 明

为使读者充分了解本书内容，书中在正文与照片中会经常提及各厂商的名称及其所有的商标，现将各商标说明列出，并感谢各厂商提供的相关资料与图片。

1．Intel、i80486DX2/DX4、Pentium 等，为 Intel(英特尔)Corp.的注册商标。

2．AMD、Am486DX2/DX4 为 ADVANCED MICRO DEVICES LTD.的注册商标。

3．Microsoft、MS-DOS、Windows、MSCDEX 为 Microsoft(微软)Corp.的注册商标。

4．Creative Sound Blaster Diagnose QCD 为 Creative Technology Ltd.(创通)的注册商标。

5．UltraSound 为 Advanced Gravis Computer Technology Ltd.的注册商标。

6．AHA-1542xx、BTC、Magic 16、Mozart、Spectrum16、U2 分别属于各注册公司之注册商标。

7．Mitsumi、NEC、Panasonic、Pioneer、Plextor、SONY、TEAC、TOSHIBA、Wearnes 分别属于各注册公司的注册商标。

8．Cdmet、HQ-9000、空中英语教室、MPC Winner 分别属于各注册公司所有。

因为所提及的产品与商标众多，在此无法一一列出，特再次说明各注册商标分别属于各注册公司所有。

# 丛书前言

电脑的魅力不但在于其高效和用于娱乐，更重要的是它始终体现着我们这个时代的脉搏。电脑技术的发展日新月异，硬件在不断升级换代，软件版本也在不断更新。这固然给用户带来了欣喜，但同时也给用户造成了压力——必须不断地学习和实践。

电脑作为一种工具，它最鲜明的特点就是用户可以自己组装、更新各种部件，使自己的电脑不断升级，以满足需要。在成千上万的电脑品牌后面，有数不清的电脑部件生产厂商在提供不同类型的零配件。当然，您在看到有更新型的部件之后，也不妨自己动手进行更换，使电脑更好地工作。但是自己动手，问题就来了。例如：如何预防、减少硬件故障的发生；在硬件故障发生后如何及时排除和修复；如何安装、升级电脑硬件；如何保证电脑可靠运行而且能更好地发挥作用等等，这些已成为众多计算机用户和广大专业维修人员十分关注的问题。《用电脑不求人系列》丛书即可帮助读者解决这些问题。这套系列丛书的最新书目如下：

- 《选用主机板不求人(第二版)》
- 《选用 SCSI 家族不求人》
- 《升级电脑不求人》
- 《装修电脑不求人》
- 《自救电脑不求人》
- 《电脑死机不求人》
- 《电脑优化不求人》
- 《急救硬盘不求人》
- 《刻录光盘不求人》
- 《架设网络不求人》
- 《电脑选购与维修不求人》
- 《设置 BIOS 不求人》
- 《VCD 光盘刻录不求人》
- 《防范黑客不求人》

组织出版这套丛书的目的是为了深入浅出地介绍各种硬件设备的规格、类型及其安装、升级的知识，并通过简单明了的图例和实际操作步骤的介绍，循序渐进地引导读者掌握各种硬件的使用方法。鉴于许多电脑用户和大中专院校学生虽具有一定的电脑基础知识，但对于机器内部各种部件到底是什么模样并不很清楚，这套丛书中提供了大量实物照片，可以帮助读者增加感性认识。另外，每章的最后一节是“问题与解答”，它可以为读者解答疑难问题、巩固所学的知识。

我们力求使本丛书突出实用性强的特点，以适合广大电脑爱好者进一步学习电脑知识的需求，帮助广大读者提高使用、维修电脑的能力。

我们希望这套丛书能成为用户使用电脑过程中的好朋友。

编者

2000 年 9 月

# 目 录

# 第一章 概 述

## 1-1 引言

根据调查显示，上网人口中只有不到一成的人有网络购物的经验，因为大家都知道网络不安全。

根据调查显示，上网人口中只有不到一成的人有防范黑客的经验，因为大家都不知道黑客的厉害。

这是不是很矛盾呢！大家都知道网络不安全，却又都没有采取加强网络安全的措施，以至于让黑客有入侵的机会。

有鉴于此，笔者奋不顾身“乔装”成黑客，混入黑客集团中“卧底”，冒着“生命危险”偷取黑客入侵惯用伎俩，然后再将这些黑客入侵的方法公诸于世，让世人免受黑客入侵。

防范黑客入侵指南在哪儿（某读者渴望地问）？远在天边，近在眼前，就是你目前看的这本书啦！

# 1-2 认识黑客

计算机黑客的种类众说纷纭，有人说是 HACKER，也有人说是 CRACKER，中文翻译更是五花八门，像是黑客、害客、骇客、怪客等，让人丈二金刚摸不着头脑。

有鉴于此，笔者林东和在此要将黑客的定义统一化，让中英文翻译能够一致，不再造成不必要的混淆。

计算机黑客可以分为下列三种：

## 一、HACKER

HACKER，笔者将它翻译成黑客，这种黑客是属于助人的黑客，主要的目的是寻找网络安全的漏洞，让网络能够更加安全地运行。

## 二、CRACKER

CRACKER，笔者将它翻译成骇客（或怪客），这种骇客是属于害人的黑客，主要的目的是通过网络漏洞偷取别人的机密资料，或是传送大量的网络垃圾，达到让网络堵塞及电脑死机的目的。

## 三、PHREAKER

PHREAKER（phone freak 的合成），指一种对电话系统极感兴趣的人。通常他们利用自己对电话系统的了解,盗用他人帐号打电话。笔者将它翻译成怪客，这种怪客也是属于害人的黑客，主要目的是通过非法电话网络入侵公司的电话总机，然后再打免费的长途电话。

本书主要的目的就是要揭发计算机黑客入侵计算机的伎俩，让你免受 CRACKER（骇客）的入侵，如果看完本书让你成为有助网络安全的 HACKER（黑客），相信这也是社会之福吧！

至于电话入侵的 PHREAKER（怪客），笔者林东和压根就瞧不起，没钱就不要打长途电话，干嘛要入侵别人电话总机去打免费电话，真是无聊透顶，所以笔者就不介绍这种黑客入侵方式了。

有关认识黑客详情，请参考第二章详尽的解说。

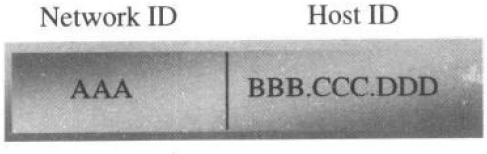
# 1-3 IP 与 PORT

所谓 IP 地址，是 Internet Protocol Address 的英文缩写，IP 地址是由 32 位所组成，并用句点（.）分成 AAA.BBB.CCC.DDD 四组数字，此四组数字是由十进制（Decimal）所组成，这四个数字的范围都介于 0～255 之间。

例如：www.yahoo.com 网址的 IP 地址是：

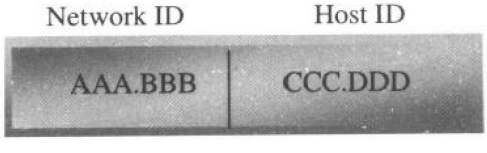

IP 地址等级有下列三类：

**一、A 类地址**



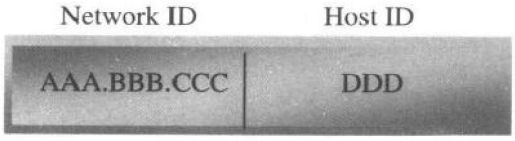

A 类地址的 Network ID（AAA）是由 1～126 所组成，每个 Network ID 拥有的 Host ID 数（BBB.CCC.DDD）高达 16 777 214 个。

**二、B 类地址**




B 类地址的 Network ID（AAA）是由 128～191 所组成，每个 Network ID 拥有的 Host ID 数（CCC.DDD）为 65534 个。

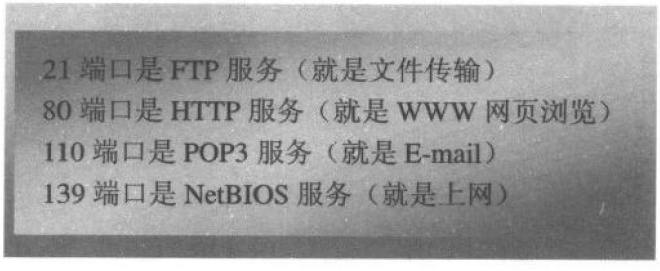
### 三、C 类地址




C 类地址的 Network ID（AAA）是由 192～223 所组成，每个 Network ID 拥有的 Host ID（DDD）为 254 个。

每台计算机虽然只有一个 IP 地址，但是却可以开启许多服务的 PORT 端口。

常见的 PORT 端口有：




有关 IP 与 PORT 的详细内容，请参考第三章的详尽解说。

## 1-4 Windows 系统入侵

只要你是使用 Windows 95/98/NT/2000 计算机上网，而且也提供资源共享的功能，那么如果你不懂得保护，你的计算机数据就如同不设防的城市一样，让黑客自由取舍。

## 一、网上邻居入侵法（见图 1-1）

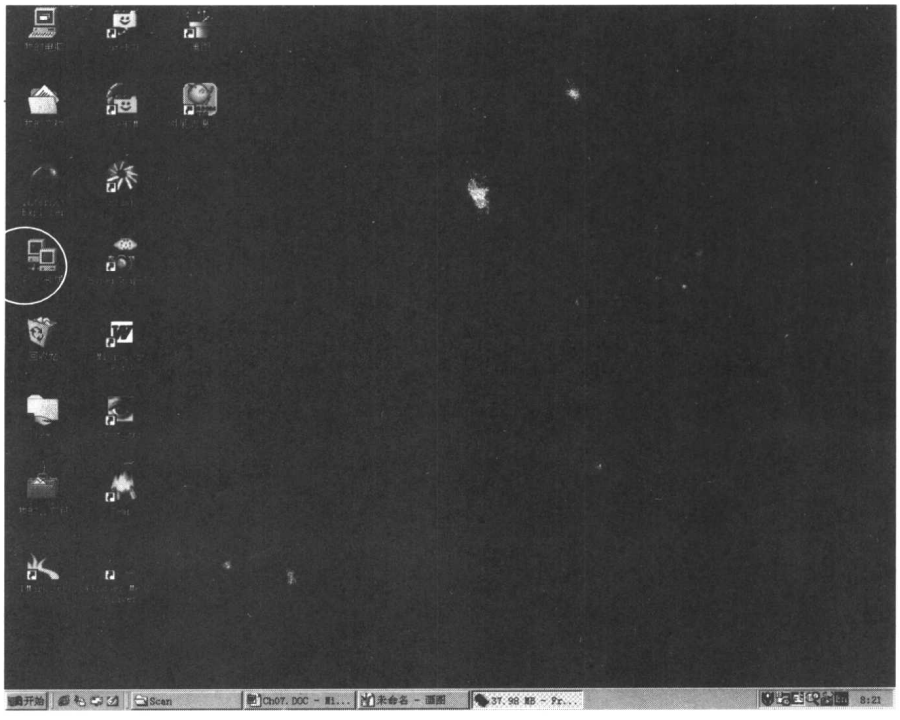


图 1-1

## 二、寻找计算机入侵法（见图 1-2）

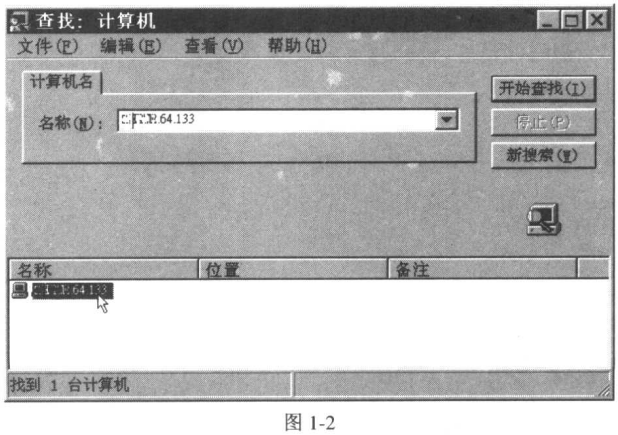



图 1-2