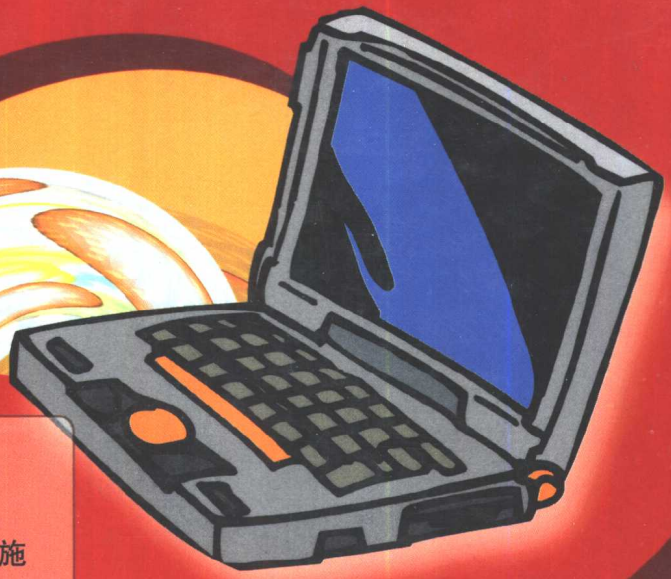
警惕免费的午餐，保护个人与公司的知识财富

读者对象：
本书是一本讲述安全使用个人电脑的普及读物，适合广大初、中级电脑用户阅读参考，既可作为普通电脑用户提高电脑安全防范意识、补充电脑安全知识的指导书籍，也可供大中专院校有关专业的在校学生作为辅助教材。



主要内容：

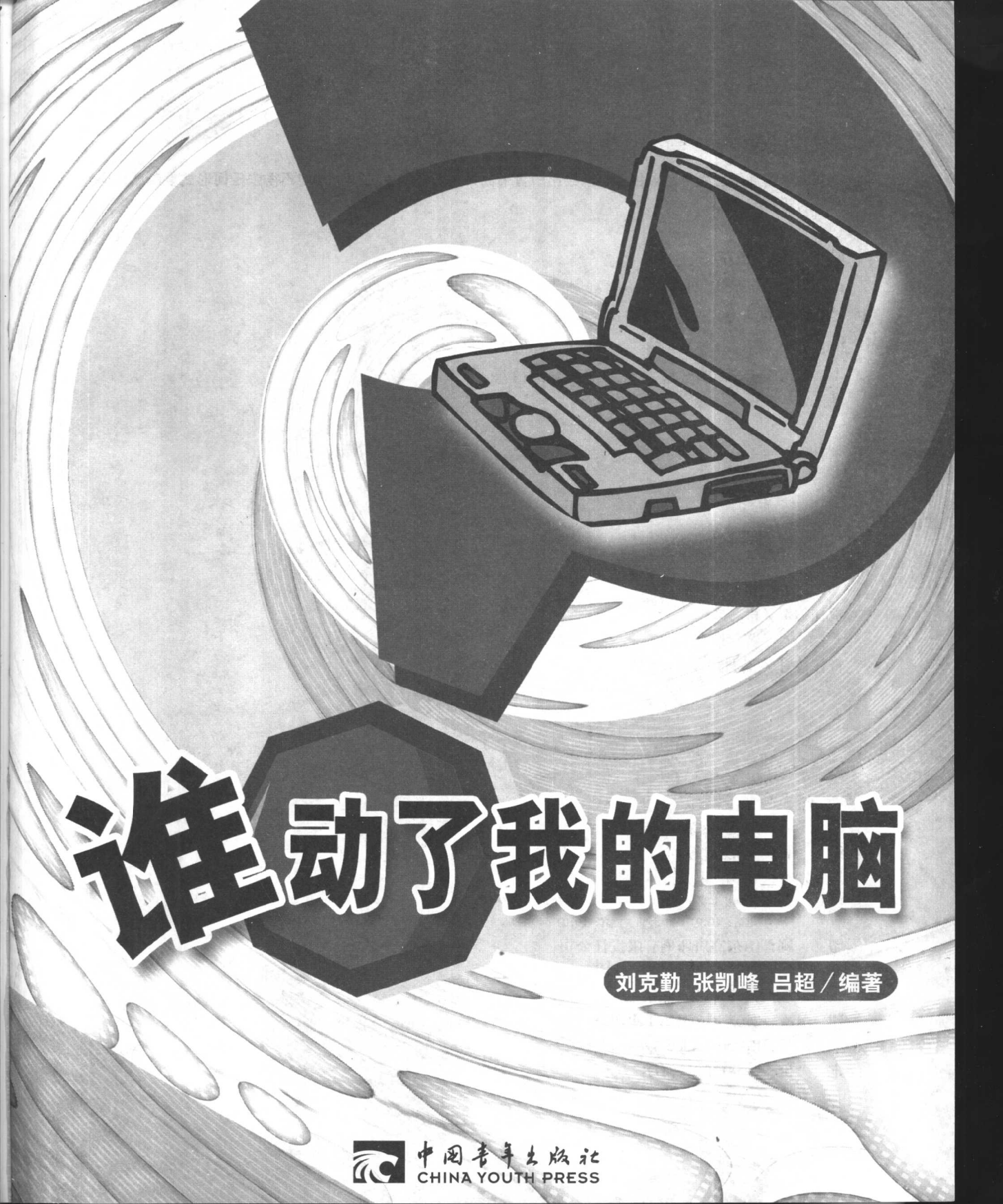
- 电脑的开机安全
- 密码设置与管理
- 数据加密与数字签名
- 数据备份与恢复
- 捍卫个人电脑隐私
- 局域网中共享资源的保护
- 安全使用 Office 办公软件
- IE 遭遇攻击后的修复
- 安全的浏览网页
- E-mail 的安全措施
- QQ 软件攻防战
- 防御可怕的木马攻击
- 计算机典型病毒防治
- 个人电脑操作安全
- 安全屏障——防火墙
- 电脑的监控与反监控

谁动了我的电脑

刘克勤 张凯峰 吕超／编著

本书附赠光盘内含各章涉及的国内外常用安全软件与相关资料

中国青年出版社



谁动了我的电脑

刘克勤 张凯峰 吕超／编著

中国青年出版社
CHINA YOUTH PRESS

（京）新登字 083 号

图书在版编目(CIP)数据

谁动了我的电脑？/ 刘克勤等编著. - 北京：中国青年出版社，2003

ISBN 7-5006-4983-5

I. 谁... II. 刘... III. 电子计算机 - 安全技术 IV. TP309

中国版本图书馆 CIP 数据核字(2002)第 105858 号

总 策 划 / 胡守文
　　王修文
　　郭　光
责任编辑 / 肖　辉
　　黄　谊
责任校对 / 王志红

书　　名：谁动了我的电脑？
编　　著：刘克勤 等
出版发行：中国青年出版社
　　地址：北京市东四十二条 21 号　邮政编码：100007
　　电话：(010) 84015588　传真：(010) 64053266
印　　刷：山东高唐印刷有限责任公司
开　　本：787 × 1092　1/16　印张：27.5
版　　次：2003 年 2 月北京第 1 版
印　　次：2003 年 2 月第 1 次印刷
书　　号：ISBN 7-5006-4983-5/TP · 295
定　　价：39.90 元（1CD）

前言

随着人类步入21世纪，电脑已经成为我们日常工作、生活中不可替代的有力工具。同时伴随着电脑的普及、网络技术的发展，人们已经不满足于“孤立”电脑的使用，而是想通过网络实现信息的交互和资源的共享。但是，任何事情都有其两面性，电脑、网络在为我们提供帮助和便利的同时，也为那些不法之徒入侵我们的电脑、盗取我们的隐私、破坏我们的数据打开了方便之门。可以说信息安全问题与能源问题、人口问题、环境问题一样，已经成为摆在人类面前需要迫切解决的问题之一。

有这么严重吗？这可能是大多数读者共同的疑问。但事实上，可能要比我们想像的严重得多。如果您是一个地地道道的电脑用户，面临这些安全问题是无疑的。如果您不经常使用电脑，那么只要您使用手机联络亲友，用MP3随身听欣赏音乐，使用数字摄像机拍摄影片，驾驶带有全球定位系统的轿车，甚至在家里使用微波炉做饭，都有可能与个人隐私和安全问题沾上边。这可不是耸人听闻，有些读者可能已经遇到过类似的问题了。

目前市面上关于信息安全、黑客攻击的书籍足以让人眼花缭乱，其中大部分都是为网络专家、安全专家那些专业人士所准备的，却很少关照电脑的普通用户，而往往电脑的初、中级用户却是安全问题的最大受害者。大部分书都沿用“从技术角度出发，由技术、原理及漏洞引出安全隐患，随之介绍防御方法和功能软件”的写作模式，这样就要求读者要对信息安全的概念有一个清楚地认识和具备扎实的计算机理论知识，显然，这不太适合广大计算机普通用户阅读。而本书立足于计算机的大众用户，紧紧抓住隐私保护与电脑安全这两个中心，以通俗的语言和清晰的表述，向广大读者介绍了计算机系统的安全知识和有关应用实例及软件实用技术，并从实际操作出发，用具体的实例引出信息安全的相关概念，力图用简单、有效的方法解决用户所面临的实际安全问题。希望通过阅读本书可以帮助读者建立起电脑隐私保护、安全防范意识及应对突发危急事件的能力。

全书共分为20章，每章一个主题，本书的一个亮点即是每个主题帮您解决一个面临的实际安全问题。具体内容涉及开机安全、密码设置与管理、数据加密技术、数据备份与恢复、个人隐私保护、局域网安全、Office办公资料的保护、浏览器的攻击与防御、安全收发电子邮件、

QQ 安全问题、木马攻击、病毒防护、电脑硬件操作安全、防火墙技术，以及监控与反监控的方法、工具介绍等。本书的另一个亮点在于提出了个人电脑隐私保护的观点，在整本书的写作中都贯穿了这一思想，目的在于提高读者自身的安全、保护意识，也许电脑已经变成了告密者，您的操作直接决定了它们到底站在哪一方？

本书是集体智慧的结晶，我们的许多研究生参加了编写工作。其中徐洪斌参加了第 1、2、5、6、8 章的编写，李莉敏参加了第 3、4、19 章的编写，张凯峰参加了第 7、10、11、13、18 章的编写，林媛媛参加了第 14、15、17 章的编写，常新苗参加了第 16 章的编写，吕超参加了第 9、12、20 章的编写工作。

本书适合广大初、中级计算机用户阅读、参考，既可作为普通电脑用户提高电脑安全防范意识、补充电脑安全知识的指导读物，也可供大中专院校有关专业的在校学生作为辅助教材。在向读者推荐本书的同时，我们也认识到计算机系统安全技术发展十分迅速，以我们的现有水平很难将所有计算机安全问题在书中全面、准确地反映出来，因此书中难免会有疏漏、错误之处，在此恳请读者及有关专家批评指正。

刘克勤

2002 年 12 月 于华北电力大学（北京）

目　录

谁动了我的电脑

第15章 木马

第16章 计算机病毒防治

第17章 其他网络攻击

第20章 监控与反监控

警惕免费午餐

近年来，Internet 在我国有了飞速的发展。上网冲浪仿佛成了当今的一种时尚。可是，网民也同现实社会中的人一样，良莠不齐。朋友们可曾遇到过这样的情况——当你正在聊天室里高谈阔论时突然被莫名其妙地“踢”出聊天室；使用从网上下载的软件后发现自己的电脑变得不那么“听话”了；最要命的情况是，当你交网费的时候发现拿到的是天文数字的账单，所有的这些迹象表明你受到了网上的非法侵害。面对着这些你无法容忍的侵害行为，许多初级网友只能暗气暗憋，毫无招架之功。不过，我劝这些朋友不要气馁。正所谓“千里之行，始于足下”，我相信在读了本书之后，你就会对电脑安全有一个初步的认识了。好了，不再讲这些空话浪费大家宝贵的时间了，现在就让我们从一个入侵实例开始，步入个人电脑安全的神秘殿堂吧！

本章主要内容：

- 我的电脑怎么了？
- 故障分析
- 模拟攻击实例

谁动了我的电脑

1.1 我的电脑怎么了?

许多网友在上网时可能会遇到这样的情况——自己刚从网上下载了一幅美丽的图片，或发现自己的电子信箱里有一封匿名邮件，打开后渐渐发觉一向对你“唯命是从”的“爱机”仿佛此刻不再听命于你。有时你明明要打开一个文本文件，可它偏偏却要打开另一个图片文件；有时你可能会发现自己的重要文件“神秘”地不翼而飞了；更糟糕的是，有时只要你一上网，电脑就会不断地重新启动，害得你无法享受冲浪的快感，而不上网时，电脑又变回了你亲密的朋友。

1.2 故障分析

面对这一系列的“不解之谜”，缺乏电脑基础知识的朋友的第一反应就是——电脑坏了。其实，电脑硬件出现故障的几率是非常小的，有的朋友自从买了电脑到几年后升级换代，都不曾光临过电脑维修部。电脑故障的大部分原因都是由于用户的不当操作或是软件本身的 Bug 所致。更何况这些故障都是在你上网的时候才发生，这一点就提醒了我们，故障肯定与网络有关。误操作亦或是软件 Bug？仔细回想一下，也不像，若是的话，故障现象应该一致，而且也不应该是时有时无的。那么，回想到所有的故障都是在你第一次打开了那张图片或那封匿名信后发生的，所以那张图片或匿名信才应该是罪魁祸首。

Bug 是对软件漏洞的一种说法。

有一些电脑基础的朋友可能马上会说：“是病毒作祟!”，的确有这个可能。在如今的网络环境中，安全机制还不是很健全，当病毒被释放到网络中的时候，你根本无法也不能预测到它的扩散能力有多么强。再加上如今的电脑病毒花样不断翻新，有的病毒可以让你拒绝服务、有的病毒可以损坏你的数据、有的病毒可以把你的 PC 变成“公用”的、而有的病毒可以让你的 PC 进入坟墓……。所以，拥有一套良好的杀毒软件（如金山毒霸、瑞星等）并定期为自己的电脑“消毒”不失为一个明智之举。但你千万不要为自己拥有一套性能优越的杀毒软件而沾沾自喜，我想告诉你的是病毒程序总是走在反病

毒工具的前面，你不要完全依赖杀毒程序为你查杀一切病毒。关于几种流行电脑病毒的机理及查杀办法，我们会在专门的章节里向你阐明，在此我们不做过多的解释。

除了电脑病毒之外，最有可能的原因就是黑客入侵。

在英文原意里，Hacker（黑客）最初的意思是指一类计算机高手，这类人有喜欢研究系统漏洞的嗜好，他们并不入侵别人的系统；而真正入侵别人系统的人被叫作 Cracker（骇客）。

其实，黑客也分为初级黑客和高级黑客，大多数的初级黑客多是利用网上提供的现成的黑客工具来入侵他人系统，此系统多是个人用户的电脑。因为多数现成的黑客工具都已被现有的杀毒工具或防火墙系统所封杀，利用这些工具入侵大型服务器系统，其成功的可能性几乎是微乎其微的。而且多数个人用户的安全意识并不是很高，至今仍有许多网友没有为自己的电脑装上个人防火墙系统。因此，个人电脑系统自然而然成了这些初级黑客的首选。而真正的黑客高手是耻于入侵个人电脑的，他们往往利用自己编写的入侵程序侵入拥有大量有用信息的服务器系统，只有这样才能满足他们的欲望。

知道了这些后，朋友们也许会问：“那么，那些初级黑客是利用什么工具入侵的我的系统呢？”其实，现有的入侵工具数量非常多，但其基本原理大都是利用木马来实现。

木马，又名特洛伊木马，它是一种基于远程控制的黑客工具，当黑客骗取你下载并执行了含有木马的程序后，它就潜入你的电脑系统，通过种种隐蔽的方式在系统启动时自动加载并在后台执行，通过客户 / 服务器模式，以“里应外合”的工作方式，达到当你上网时控制你的电脑，窃取你的密码、游览你的硬盘资源，修改你的文件或注册表、偷看你的邮件等目的。

在客户 / 服务器模式中，我们将请求服务的一方称为客户，将提供某种服务的一方称为服务器。客户提出请求发送给服务器，服务器响应客户请求并提供相应的服务。

基于这种模式的应用程序都由客户端程序和服务器端程序组成，木马就是这样的一种程序。发送给别人执行的就是服务器端程序，而自己则利用客户端程序与服务器端程序取得联系，从而获得相应的“服务”。

1.3 模拟攻击实例

了解了木马的概念后，你一定会对木马产生极大的好奇感吧。好吧，那就让我们以一个实际的木马为例，模拟一次木马攻击，让你见识一下木马的威力。（此实例仅供我们学习之用，若以此攻击其他网友，所产生的一切后果，笔者概不负责。）

我们此次模拟所用的木马程序叫做“网络精灵”，目前它的最高版本为 3.0 版，相信在网上你一定能够找到它，赶快下载一个吧。（不过下载的时候一定要打开个人防火墙呦，否则，下载木马却中了别人的木马，那真是一种讽刺呀。）为了让大家看清楚木马的整个工作过程，我们这次在局域网的环境中模拟，此时木马的工作原理等同于 Internet 环境。

好了，首先将下载的木马解压缩（不要告诉我你不会解压缩，若真的不会，在网上找找相关资料学习一下吧）。解压后，你会在解压的文件夹内找到 netmonitor.exe 和 netspy.exe 两个文件。其中，netmonitor 为“网络精灵”的客户端程序，也就是你用来控制别人系统的工具，而 netspy 则为“网络精灵”的服务器端程序也就是你要发送给别人，要别人来运行的程序。你可千万不要在你的机器上运行它呀，否则你就会为自己的电脑“种”上木马。

下一步就是要把“网络精灵”的服务器端程序 netspy 发送给你想控制的电脑。在这里，我们直接把 netspy 拷贝到另一电脑 C 盘根目录下。当然，这在实际的 Internet 环境中是不可能做到的。现实中，黑客们经常将木马的服务器端程序与另一个应用程序文件（如当今流行的游戏或好看的美眉照片）利用文件合成软件进行合成，再配上一个好看的图标，然后哄骗我们这些善良的网友下载这样的程序。这样，大部分网友都不会注意到木马的存在。当然，这也要以对方的系统中没有安装防火墙为前提，如果有防火墙，“网络精灵”就会被封杀在系统之外。由此可见防火墙在个人电脑安全领域中的重要性。如果不幸你没有防火墙，那么，只要你运行了刚刚下载的程序，“网络精灵”就会悄悄地潜入你的系统，而且，在你每次启动系统时，它都会自动加载并在后台运行，即使在 Windows 2000 / XP 的任务管理器中也不能找到它的踪影。怎么样，够隐蔽吧！

为了清楚地向朋友们展示 netspy 程序是如何在你的系统中隐藏的，我们这里没有将之合并到其他文件中，试着在目标计算机上（没有 netmonitor 程序的计算机）运行一下 netspy 程序（双击图标），你会惊奇的发现，它的图标“神秘”的消失了。那么它到底“跑”到哪里去了呢？我们用 Windows 的查找工具来查找一下，单击“开始/搜索/文件或文件夹”，出现图 1-1 所示的查找结果。

此时，我们发现它自动地“跑”到了 C:\WINDOWS\SYSTEM 目录下。这是在 Windows 98 系统上的结果，若是 Windows 2000 / XP 结果会有所不同。好，我们进入 C:\WINDOWS\SYSTEM 目录看一看，结果正如我们所料，它确实在那里。

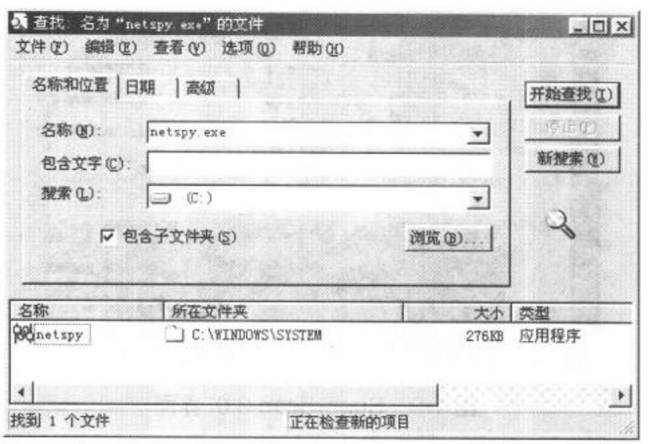


图 1-1　Windows 查找工具

好了，此时我们的木马“网络精灵”已“安全”潜入目标计算机。接下来我们要做的工作就是端口扫描。

如果我们把 Internet 比作路，而你的个人电脑比作路边的房屋，那么端口就是你房屋的门，只有通过门，你才能从屋里上路。我们的电脑可以有 256×256 扇门，即从 0 到 65535 号，每一个号都是一个端口。

什么？你问为什么要进行端口扫描？答案当然是要从端口进入你的电脑。由于我们的电脑有 256×256 个端口，但只有当某一端口被打开时，黑客才能从这一端口进入你