新电脑生活丛书

网络安全

焦赢洲

本丛书累计600 000册销售

上海科学技术出版社

新电脑生活丛书

网络安全

焦赢洲 编著

上海科学技术出版社

图书在版编目(CIP)数据

网络安全 / 焦赢洲编著. — 上海：上海科学技术出版社，2002.4
(新电脑生活丛书)
ISBN 7-5323-6481-X

Ⅰ.网… Ⅱ.焦… 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（2002）第 014167 号

上海科学技术出版社出版、发行
(上海瑞金二路 450 号 邮政编码 200020)
上海书刊印刷有限公司印刷
新华书店上海发行所经销
开本 787 × 1092 1/32 印张 2.25 字数 50 000
2002 年 4 月第 1 版 2002 年 4 月第 1 次印刷
印数 1—6 000
ISBN 7-5323-6481-X/TP · 230
定价：10.00 元

目　录

新电脑生活丛书

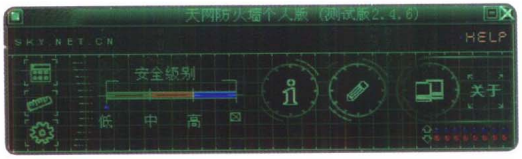
网络安全

焦嬴洲 编著

上海科学技术出版社

关于本书

近年来，随着网络技术的高速发展，上网已经成为一种必需，它给我们的生活、学习、娱乐都带来了很大的方便。但是，在这缤纷的因特网背后，隐藏着许多不安全的因素：利用网络蓄意攻击他人的所谓“黑客”，在网上传播且无孔不入的病毒，以及个人隐私的泄漏，等等，不胜枚举。因此网络安全也就为越来越多的网友所关心，尤其是对于那些上网的新手而言，学会在网上如何进行自我保护的确是迫在眉睫了。



本书通过一些具体的实例，在介绍因特网上常见黑客攻击方法的同时，详细地介绍了两款较为知名的个人防火墙软件——天网防火墙和 Sygate Personal Firewall Pro 的具体使用方法。读者通过阅读本书，可以轻松地掌握这两款软件的安装和使用，并且在此基础上，能够针对自己电脑所处的网络环境和工作环境来进行个性化的设置，从而有效地防止黑客攻击和病毒的入侵。这样，您就可以高枕无忧地在网络的信息海洋中畅游，真正享受网络带来的乐趣了。

本书提及的键名、菜单、命令、按钮、选项，以及作者输入的内容均以黑体字在文中标示。文中的单击指按鼠标左键一下，双击指连续按鼠标左键两下，单击右键指按鼠标右键一下。键名＋键名指同时按下此两键。本书的章节以页脚的不同渐变色加以区分，技巧和注意事项用楷体字加色块标示。

读者对本丛书有何意见和建议，欢迎来信：上海市瑞金二路 450 号，邮政编码200020，电脑编辑室，或访问上海科学技术出版社精品电脑图书频道，网址 http://www.sstp.com.cn/computer.htm。

目　录

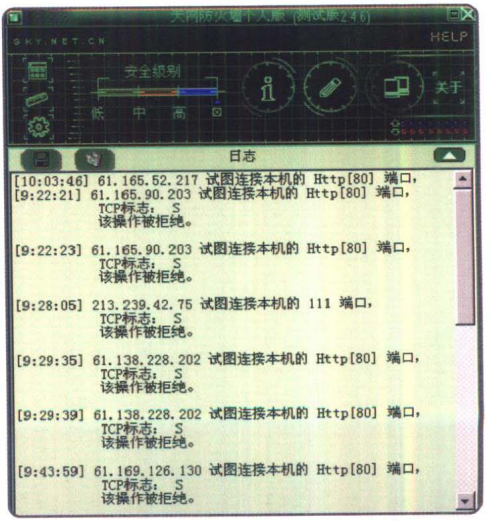
天网防火墙的安装

天网防火墙个人版是一款给个人电脑使用的网络安全程序。它把网络分为本地网和因特网，可以针对来自不同网络的信息，来设置不同的安全方案，并且可以根据您自己设定的安全规则来监视网络，提供强大的访问控制、应用选项、信息过滤等功能。使用它可以比较方便地帮助您抵挡黑客的入侵和攻击，防止信息泄露。

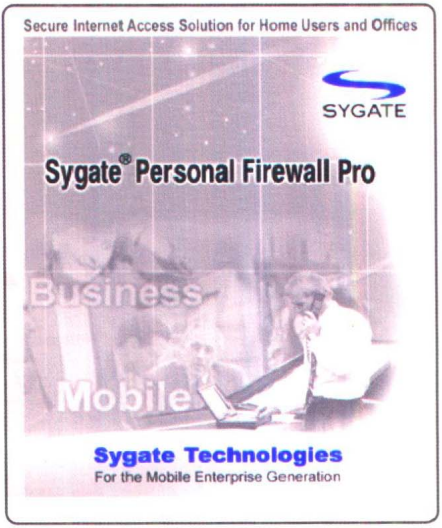
网络安全知识简介

1 什么是网络安全

谈到网络安全，也许很多个人会说，我又不是什么大的官方网站或企业网站，黑客们怎么会对我这种无名之辈的电脑感兴趣呢？如果这样想的话，那您就错了。黑客的攻击很多时候并不只是针对官方网站或者企业网站的，他们经常使用地址扫描软件对某一地址段进行大规模的端口扫描，这些程序的扫描速度是非常快的，它们并不是针对一个或几个特定的目标网站，它们只是机械地重复寻找每一个地址上所有正打开着的端口。所以从这一点来看，您个人和官方网站、企业网站受到黑客攻击的概率是相同的。



网络是信息的海洋，其浩瀚的信息量是如此地诱人，但因为其特殊的隐蔽性及网络使用者的道德素养参差不齐，法制观念的淡泊，所以很多道德低下的网民经常以肆意破坏别人的系统为乐趣，甚至为了自己私利，盗取别人的各种密码及个人隐私信息，如上网帐号和密码，信用卡帐号和密码，电子邮箱帐号和密码，等等。



现在官方和企业网站也日益重视网络安全的重要性，通过购置硬件防火墙、软件防火墙，及时地修补系统的各种漏洞，进行正确的网络安全配置，寻找专业的网络安全公司进行安全检测等措施，黑客们已经很难像以前一样，通过一些简单的手段即可直接攻击官方网站或企业网站了。这时，黑客们往往把目光转向个人用户，因为攻击个人用户要比突破严密防守的官方或企业网站容易得多。比如黑客们通过攻击个人用户来获取密码信息，而这些密码信息可能在攻击官方或企业网站是很有用处的；或者是通过攻击获取个人用户的控制权来骗取官方或企业网站防火墙的信任，等等。在去年的微软黑客入侵事件里，黑客正是通过攻击微软公司一名员工的电脑，最后把蠕虫病毒突破置入到微软的主机系统，导致微软很大一部分产品源码被窃取，造成了重大损失。

什么是防火墙

防火墙就是一个位于电脑和它所连接的网络之间的软件，该电脑流入、流出的所有网络信息均要经过其严格的检查，若不符合其设定的安全标准，则无法通过。

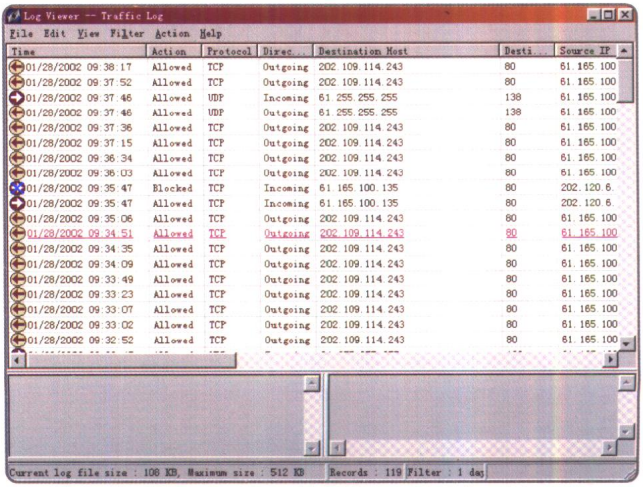
2 常见的黑客攻击手段和途径

● 窃取您的主机信息

任何一台在因特网上的电脑都会有一个唯一的IP 地址。通常来说，IP 地址有两种，一种是静态的IP 地址，如您通 DSL、光纤或其他高速连接方式上网，您的IP 地址很可能是静态的，即永远不变的地址；另一种是动态变化的IP 地址，比如您通过调制调解器拨号上网，通常就是动态变化的IP 地址，该动态地址是由供您接入的服务商ISP 来分配的。而这个 IP 地址就是黑客们攻击您主机的唯一线索，黑客们一般是通过发送TCP数据包来探测您的IP 地址，然后再通过IP 地址获取您的主机信息，还可以通过Netbios 来获得您的主机名、登录名、工作组等信息。

● 扫描您的主机端口

在您的主机连入因特网后，会打开许多通讯端口，通常在这些端口中有一部分是您与外界通讯所必须的，如您浏览网页、使用QQ聊天等都会打开一些通讯端口，而另一部分端口是系统的一些网络服务程序自动打开的，如Web 服务器的 80 端口、Ftp 服务器的 21 端口、Windows 98 的 139 端口、Windows2000 的远程接入 3389 端口，等等。黑客们通常在确定 IP 地址后，会扫描这些端口，或者集中扫描某一个IP 地址段开放某一端口的所有地址，然后根据扫描端口的结果来推断您的操作系统及Web、Ftp 等服务器的类型，以及开通了哪些服务。

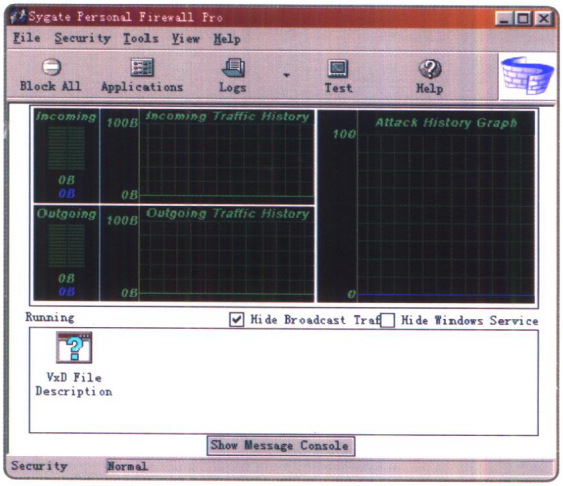


● 利用您的系统漏洞

由于很多操作系统和应用软件的开发过程中没有过多地考虑到安全问题，这就造成了很多的安全漏洞，如著名的IIS服务器的Unicode漏洞，Windows98中的ICMP包溢出漏洞，Windows 2000中文版里的输入法漏洞，Linux和Unix系统平台下著名的Bind漏洞，等等，这些安全漏洞可以使黑客很轻易地窃取您的信息或控制您的主机。

● 邮件攻击

邮件攻击是指黑客们通过电子邮件向您发送木马程序、病毒或一段带有攻击特征的特定Html代码。例如通过一段特定的Html代码，可以在您打开邮件的时候，把您的主机信息记录并发送给黑客，如果利用了IE一些版本的漏洞，甚至可以通过这些漏洞对您的文件系统进行读写操作。



● 木马攻击

木马程序一般是通过电子邮件或捆绑在一些下载的可执行文件中等途径来传播的，通常通过一些提示诱使您运行它们，然后潜伏到您系统中，并且在运行后自我销毁，然后利用各种技术手段进行简单或复杂的隐身，接着发送相关信息给黑客，以等待黑客的响应。木马程序的危害性在于它对电脑

系统强大的控制和破坏能力，可以窃取密码、控制系统操作、进行文件读写，等等。一个功能强大的木马程序一旦被植入您的电脑，黑客就可以像操作自己的电脑一样控制您的电脑，甚至可以远程监控您的所有操作。如 Sub7、BO2000、冰河等木马程序都具有强大的控制功能。

3 防范方法和工具

* 为了防范黑客扫描您的 IP 地址，隐藏您的 IP 地址不让别人探测到，最简单实用的方法是使用如天网防火墙等防火墙软件，从而有效地防止黑客扫描您的 IP 地址。

* 对于黑客对您电脑端口的探测，也可以使用反扫描的软件。现在反扫描的软件主要两种，一种是伪装型的，即这个程序伪装打开所有的常用端口，这样黑客扫描后会得到一个错误的结果，并且程序会对黑客的扫描进行记录；另一种是警示型的，即程序只能监视黑客的扫描，并且发出预警信息，但不能阻止扫描。然而这两种反扫描的软件都无法对黑客的扫描行为进行拦截，只有使用防火墙软件才可以达到这个目的，通过对防火墙进行一定规则的设定，完全可以拦截黑客的扫描行为。

* 防御系统漏洞攻击的方法就比较简单了，只要及时关注最新漏洞的报告情况，最快地为已经发现的漏洞打上补丁（对程序的一些不完善或不安全的部分进行改进的小程序）就可以了。但是，对于您个人而言，显然不可能像专业的网络安全人员一样天天关注着最新漏洞发现的情况，并及时地修补它。那该怎么办呢？没关系，有些防火墙软件就提供了漏洞扫描修补功能，如后文中将要介绍的天网防火墙就有这个功能，并且可以通过在线的漏洞资料库的更新，以最快速度发现并且修补您的系统漏洞。

* 至于邮件攻击，您除了不要轻易打开陌生邮件和一些带有诱惑标题的邮件之外，还可以采取安装防火墙、采用邮件加密、安装一些防病毒、防木马的软件等方法来进行防范。

* 木马的防范相对复杂些。现在的防火墙软件可以过滤掉木马程序与黑客之间相互联系的数据包，使得大多数木马程序无法与黑客联系。防火墙的这种过滤方式不仅适用于TCP数据包，还能够阻止UDP、ICMP等其他IP数据包的传输，这样即使木马植入成功，黑客也是无法进入您的系统的，因为防火墙把攻击者和木马程序分隔开来了。尽管如此，对于一些技术高明的木马程序，防火墙有时也是无能为力的，如寄生在HTTP端口上的木马，或者与木马正常控制程序相反的木马，它是通过木马程序向外面的端口发送数据，任何防火墙都不可能阻塞这种数据请求，要不然整个系统就不能上网浏览网页了。这时就需要您自己对防火墙的规则进行高级设置了，这点将在后文中具体向您介绍。

天网防火墙的主要功能和特点

● 严密的实时监控

天网防火墙能对所有来自外部机器的访问请求进行过滤，发现非授权的访问请求后立即拒绝，随时保护您系统的信息安全。

● 灵活的安全规则

天网防火墙设置了一系列安全规则，允许特定主机的相应服务，拒绝其他主机的访问要求。您还可以根据自己的实际情况，添加、删除或修改安全规则，保护本机的安全。

● 应用程序规则设置

天网防火墙具有对应用程序数据包进行底层分析拦截的功能，它可以控制应用程序发送和接收数据包的类型、通讯端口，并且决定拦截还是通过。

● 详细的访问纪录

天网防火墙可显示所有被拦截的访问记录，包括访问的时间、来源、类型、代码等都详细地记录下来，您可以清楚地看到是否有人侵者想连接到您的机器，从而制定更有效的防护规则。

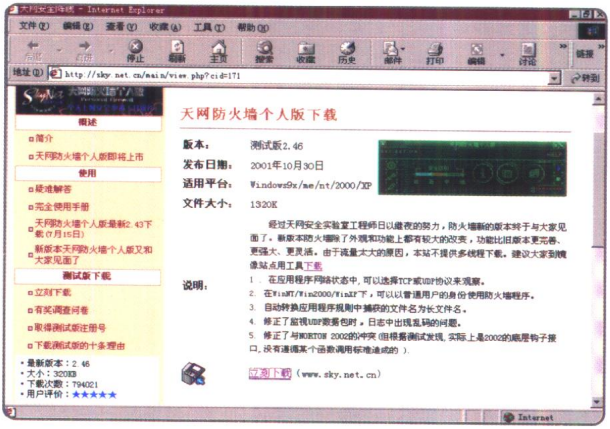
● 完善的报警系统

天网防火墙设置了完善的声音报警系统，当出现异常情况的时候，系统会发出预警信号，从而让您做好防御措施。

天网防火墙的下载

为了能够让用户可以先体验一下天网防火墙的功能和用途，充分享受一下在网上冲浪高枕无忧的那种惬意和快感，众达天网公司在其官方网站上提供了天网防火墙测试版的免费下载，您可以自行到因特网上去下载。

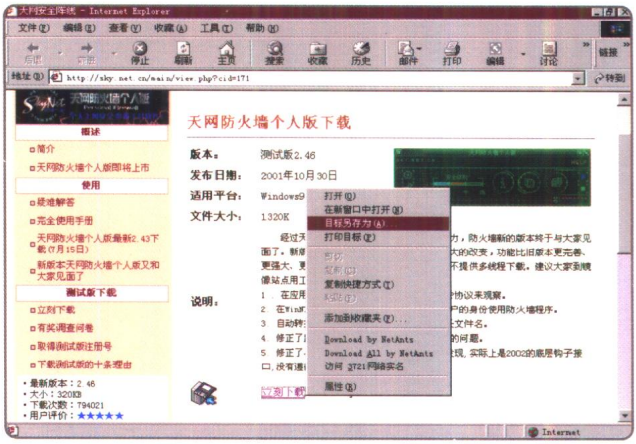
* 本书采用的天网防火墙测试版的版本是2.4.6，文件大小是1.25M，下载的网址为：http://www.sky.net.cn/main/view.php?cid=171。



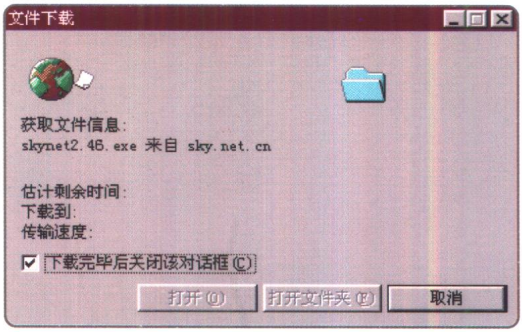
其他下载地址

因为该软件的应用比较广泛，所以在其他网站如PCHOME也提供了下载，具体地址是：http://download.pchome.net/internet/safe/381.html，如果下载链接更新了的话，可以在软件下载框中输入天网防火墙，然后单击搜索进行查找，一般情况下很快就能找到其最新下载地址。

* 在打开的网页上提供的下载链接立刻下载上单击鼠标右键，在弹出的快捷菜单中选择**目标另存为**命令。



* IE自动探测要下载的文件的大小和地址。



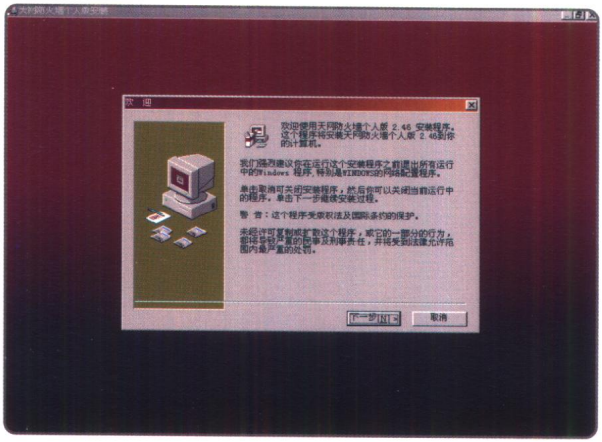
* 在弹出的**另存为**对话框中，设置用于保存下载文件的文件夹和保存的文件名，例如选择保存在**桌面**上，文件名为skynet2.46.exe，然后单击**保存**按钮。

* IE开始自动下载，并且将下载好的文件保存到刚才设置的文件夹中。

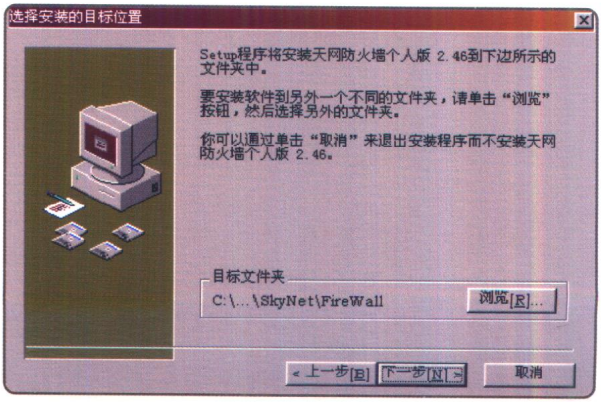
天网防火墙的安装

* 双击桌面上的 skynet2.46 文件，就可以进行天网防火墙测试版的安装了。

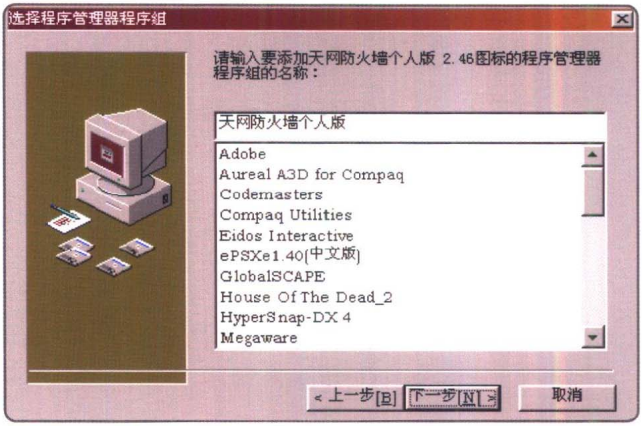
* 进入天网防火墙测试版的安装主界面后，单击**下一步**按钮。



* 接下来选择天网防火墙测试版的安装目录，建议使用默认的安装目录，直接单击**下一步**。



* 选择天网防火墙测试版的程序组名称和位置。建议采用默认名称和位置，直接单击**下一步**。



* 单击**下一步**按钮，结束安装设置，开始复制安装文件。