网络安全技术应用丛书

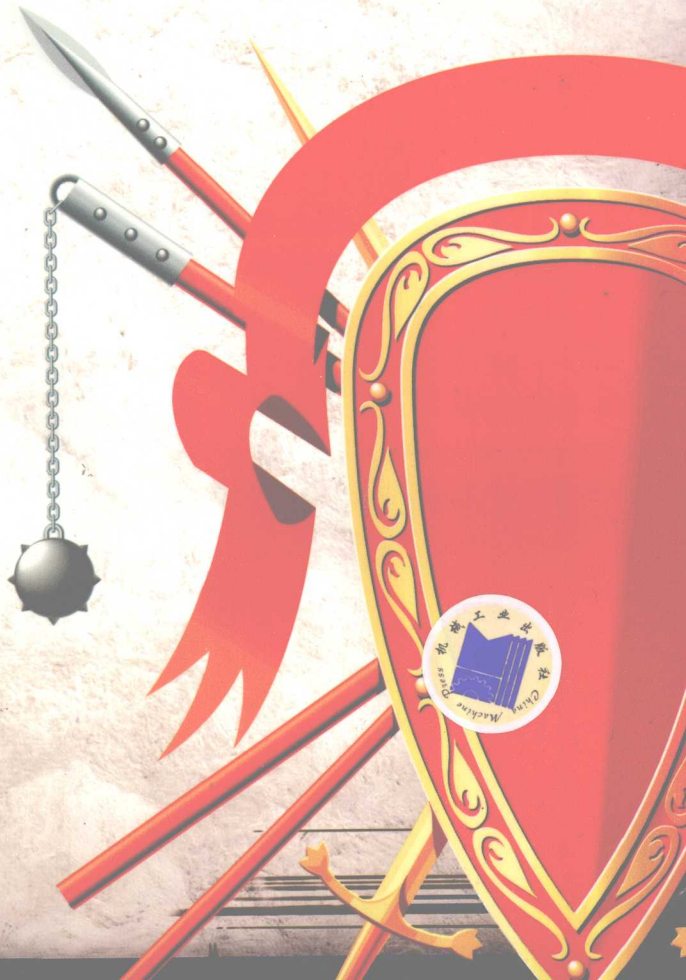
畅销书《杀破狼》作者团队最新力作！

铜墙铁壁
——黑客防范技巧与工具

武新华　刘 岩　段玲华　等编著

- Windows系统漏洞及防范措施
- 木马和间谍软件的伪装与查杀
- Web攻防实战演练
- 电子邮件攻防实战
- 后门与自身防护技术
- 网络代理与恶意进程清除
- 数据备份与恢复
- 打好网络安全防御战

附赠超值多媒体语音光盘



机械工业出版社
CHINA MACHINE PRESS

网络安全技术应用丛书

铜墙铁壁——黑客防范技巧与工具

武新华　刘 岩　段玲华　等编著

机械工业出版社

本书紧紧围绕黑客防范技巧与工具展开，在剖析用户进行黑客防御中迫切需要用到或想要用到的技术时，力求对其进行“傻瓜式”的讲解，使读者对网络防御技术形成系统了解，能够更好地防范黑客的攻击。全书共分为 11 章，主要内容包括：Windows 系统漏洞防范，木马和间谍软件的伪装与查杀，Web 攻防实战演练，QQ 与 MSN 的攻击与防御技术，电子邮件攻防实战，后门与自身防护技术，网络代理与恶意进程清除，全面提升自己的网络功能，数据备份与恢复，打好网络安全防御战等。

本书内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

图书在版编目（CIP）数据

铜墙铁壁——黑客防范技巧与工具/ 武新华等编著. —北京：
机械工业出版社，2009.6
（网络安全技术应用丛书）
ISBN 978-7-111-26656-3

Ⅰ. 铜… Ⅱ. 武… 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（2009）第 041019 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：丁 诚 吴鸣飞
责任编辑：吴鸣飞
责任印制：洪汉军
三河市国英印务有限公司印刷
2009 年 6 月第 1 版 · 第 1 次印刷
184mm × 260mm · 24.5 印张 · 604 千字
0001—4000 册
标准书号：ISBN 978 - 7 - 111 - 26656 - 3
ISBN 978 - 7 - 89451 - 057 - 0（光盘）
定价：49.00 元（含1DVD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294 68993821
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379753 88379739
封面无防伪标均为盗版

前　言

随着社会各行各业对网络技术依赖性的不断增强，人们在体验网络所带来的极大便利的同时，黑客入侵和网络安全问题也同样在困扰着网络的发展，如僵尸网络（Botnet）、网络钓鱼（Phishing）、木马及间谍软件、零时间威胁、熊猫烧香、网站挂马事件、木马产业链的曝光等，更使得网络安全问题成为大家关注的焦点。

由于互联网本身的设计缺陷及其复杂性、开放性等特点，网络的安全性已成为阻碍信息化进程的重要因素，其影响已从互联网领域逐步扩大到政府、通信、金融、电力、交通等应用和建设领域。网络安全问题已引起了全世界的密切关注，黑客的恶意行为已成为全球新的公害。

或许大家都曾碰到过这样的情况，正当自己为精彩的网页着迷时，突然硬盘狂响不止，最后发现所有的程序都不能运行了；正在给网友写 E-mail 时，突然弹出一个对话框，上面写着“我是幽灵，我要毁了你的电脑!”；正在聊天室里与网友聊天时，突然弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机；在登录 QQ 时却突然提示密码错误，试遍所有可能的密码却依然不能通过，这时才发现自己的 QQ 密码被盗了。

因此，大家必须采取有力措施加强网络的自身安全防护性能，以有效抵抗入侵和攻击破坏。但随着攻击手段的日趋复杂，有组织、有预谋、有目的、有针对性、多样化攻击和破坏活动的频繁发生，攻击点也越来越趋于集中和精确，攻击破坏的影响面不断扩大并产生连环效应，这就势必需要构筑一种主动的安全防御，才有可能最大限度地有效应对攻击方式的变化。

写作本书的目的主要是通过介绍黑客的攻击手段和提供相应的主动防御保护措施，使读者能够循序渐进地了解黑客入侵防御的关键技术与方法，提高安全防护意识，在实际遇到黑客攻击时能够做到“胸有成竹”。希望读者能够运用本书介绍的知识去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

本书特别注重实例的讲解，针对每一种攻防手段，都结合实例来进行介绍，并紧紧围绕黑客的“攻与防”这一主线，告诉读者如何建立个人电脑的安全防护措施，使自己远离黑客攻击的困扰，确保自己电脑数据的安全。

本书通俗易懂、图文并茂，即使是电脑新手也能无障碍阅读；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，让用户“先下手为强”；攻防互参的防御方法，全面确保用户的网络安全。

本书具有如下特色：

- 讲解从零起步，由浅入深，步步深入，通俗易懂，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 理论和实例相结合，实用性强，并配以大量插图和配套光盘视频讲解，力图使读者能够融会贯通。
- 介绍大量的小技巧和小窍门，可使读者节省大量宝贵的摸索时间。
- 重点突出，内容丰富，操作步骤详细，并附有大量的操作实例，读者可以一边学习，一边在电脑上操作，做到即学即用、即用即得，快速学会操作方法。

本书在编写的过程中，得到了许多热心网友的支持，部分参考了来自网络的资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

参与本书编写的人员有武新华、刘岩、段玲华、杨平、李防、李秋菊、陈艳艳、李伟、冯世雄、孙世宁、张晓新等。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

最后，须要提醒大家的是：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中所介绍的黑客技术对别人进行攻击，否则后果自负。

编　者

目　录

第1章

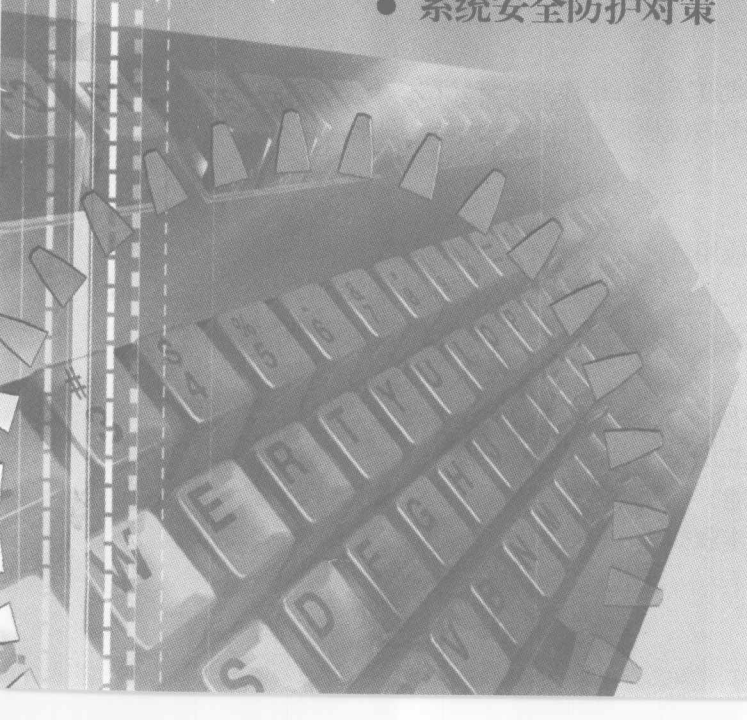
Windows 系统中的漏洞

本章精粹

通过本章的学习，读者可了解到 Windows 操作系统存在的安全隐患、黑客常用的入侵方式，以及系统安全防护的一些简单对策，对如何保护系统的安全进行初步了解，为掌握黑客防御技术奠定坚实的基础。

重点提示

- **Windows 系统的安全隐患**
- **Windows 操作系统中的漏洞**
- **黑客常用的入侵方式**
- **系统安全防护对策**



Windows 操作系统是目前应用最广泛的操作平台，随着它的更新换代，其系统安全性也逐渐提高，但安全漏洞是难以彻底根除的，黑客常常利用这些漏洞对计算机实施攻击。所谓“知己知彼，百战不殆”，要想全面防止黑客的入侵，首先需要了解 Windows 操作系统中存在的一些安全漏洞和黑客攻击这些漏洞的常用方法，并掌握一些基本的安全防护策略。

1.1 Windows 系统的安全隐患

操作系统是硬件、网络与用户的一个接口。不管用户在上面使用什么应用程序或享受怎样的服务，操作系统一定是必不可少的。随着互联网的普及，网络用户的逐渐增多，由此带来的安全问题也威胁着计算机的安全，而 Windows 操作系统本身具有的漏洞，常常为黑客们的入侵行为提供了便利之门。

1.1.1 Windows 操作系统中的安全隐患

在 Windows 操作系统中，主要存在下列安全隐患。

1．代码庞大复杂，代码重用的现象比较严重

通常情况下，程序中的 Bug 和程序的大小是成正比的。但由于 Windows 操作系统的代码量非常庞大，难免存在一些错误，而且新版本的操作系统在继承原版本重要核心代码的同时，不可避免地又继承了其原代码中存在的 Bug。

2．盲目追求易用性和兼容性

Windows 操作系统为了增强其功能，过多地支持一些程序，默认支持的程序越多，就越容易给黑客以可乘之机，并造成系统中出现关联、兼容性等一些出乎意料的问题。

3．无法辨别“/”和“\”

在 Windows 操作系统下一般使用“\”表示目录，但使用“/”系统也可接受，这就有可能会导致在编写 ASP、PHP 以及在编写 Web 服务器之类的程序时，混用“/”和“\”而对 Web 上级目录的越权访问。

4．设备文件名问题

Windows 操作系统的很多设备可以通过字符链接作为文件访问。有些程序在编写时，往往在防止对任意驱动器进行访问的控制手段模块设计上考虑不周。例如，使用“\.D:”这样的方式即可访问 D 盘。

5．注册表庞大而复杂

Windows 操作系统注册表中包含了应用程序和计算机系统的配置、系统和应用程序的初始化信息、应用程序和文档文件的关联关系、硬件设备的说明、状态和属性以及各种状态信息和数据等。由于注册表过于庞大和复杂，因此 Windows 操作系统很容易出现漏洞。

6．系统的默认设置

Windows XP 系统为了提高易用性所采用的许多默认设置，也为用户增添了更多的风险。例如，为了让网络上的用户只需点击几下鼠标就可以实现文件共享，Windows XP 系统加入了一种称为“简单文件共享”的功能，但同时也打开了许多 NetBIOS 漏洞。

关闭简单文件共享功能的具体操作步骤如下：

步骤1 双击【我的电脑】图标，即可打开【我的电脑】窗口。在其中选择【工具】→【文件夹选项】菜单项，即可打开【文件夹选项】对话框，如图 1-1 所示。

步骤2 选择【查看】选项卡，在【高级设置】选项区中取消勾选【使用简单文件共享（推荐）】复选框，如图 1-2 所示。

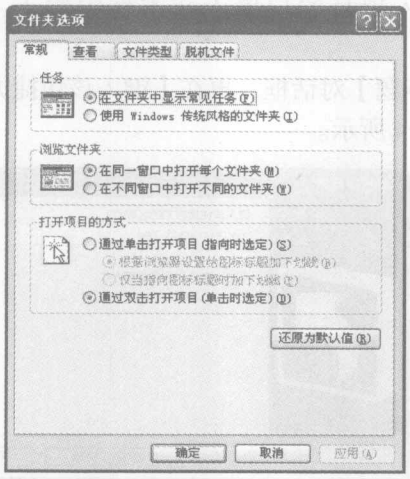


图 1-1 【文件夹选项】对话框

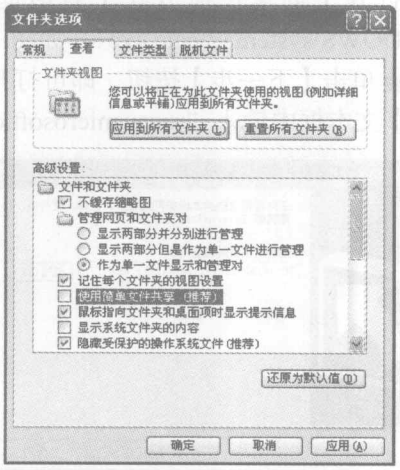


图 1-2 取消【使用简单文件共享（推荐）】复选框

7．Guest 账户

Guest 账户即来宾账户，它可以访问计算机，但会受到一定的限制。不幸地是，Guest 也为黑客入侵打开了方便之门。如果不需要用到 Guest 账户，最好禁用它。

8．Administrator 账户

Windows NT 系统有一个内建的系统管理员账号 Administrator。这个账号对整个系统拥有最高级别的控制权。在 Windows XP 系统中，这个账号被隐藏了起来，而且该账号密码是在安装操作系统时输入的。可能很多人并没有意识到这一点，因此并没有给 Administrator 账号设置密码。在这种情况下，只要有人通过网络或直接接触到用户的电脑，该用户的系统和数据就危险了。因此，如果系统中该账号密码为空，最好给这个账号设置一个密码。

9．WSH

WSH 对象非常强大，它的系统脚本引擎是默认安装的，在 IE、Office 等软件中被广泛支持，IE、Office 中的许多漏洞都与之有关。

10．系统权限分配繁冗

Windows 2000/XP 系统中几乎每一个对象、注册表项、设备等都可以设置权限，这么庞大的访问控制列表，用户自然无法一一审核，因此，其中的很多都可以被用来作为后门。

11．多余的服务

为了方便用户，Windows 操作系统还默认启动了许多不一定要用到的服务，同时也打开了入侵系统的后门。

1.1.2 Windows 操作系统中的 Bug

通常情况下，Windows 操作系统中的小 Bug 并不会给系统带来危害，但某些 Bug 很可

能会被黑客利用，从而危及系统的安全。下面简单介绍 Windows 操作系统中的 Bug，以引起用户的注意。

具体的操作步骤如下：

步骤1 在桌面上单击鼠标右键，在弹出的快捷菜单中选择【新建】→【快捷方式】菜单项，即可打开【创建快捷方式】对话框，在【请键入项目的位置】文本框中输入“C:\WINDOWS\system32\calc.exe”，如图 1-3 所示。

步骤2 单击【下一步】按钮，即可打开【选择程序标题】对话框，再在【键入该快捷方式的名称】文本框中输入“www.microsoft.com”，如图 1-4 所示。

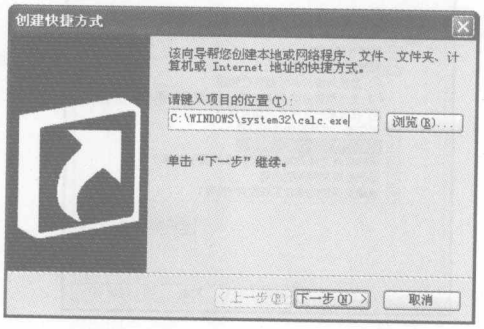


图 1-3 【创建快捷方式】对话框

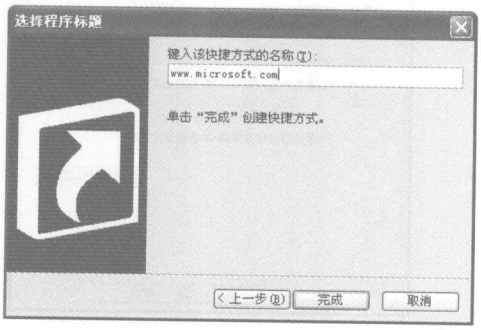


图 1-4 【选择程序标题】对话框

步骤3 单击【完成】按钮，即可完成创建。此时，桌面上将出现一个快捷方式图标。

步骤4 在 IE 浏览器地址栏中输入“www.microsoft.com”之后，即可看到此时网页并没有跳转到 Microsoft 主页中，而是打开了系统自带的计算器，如图 1-5 所示。

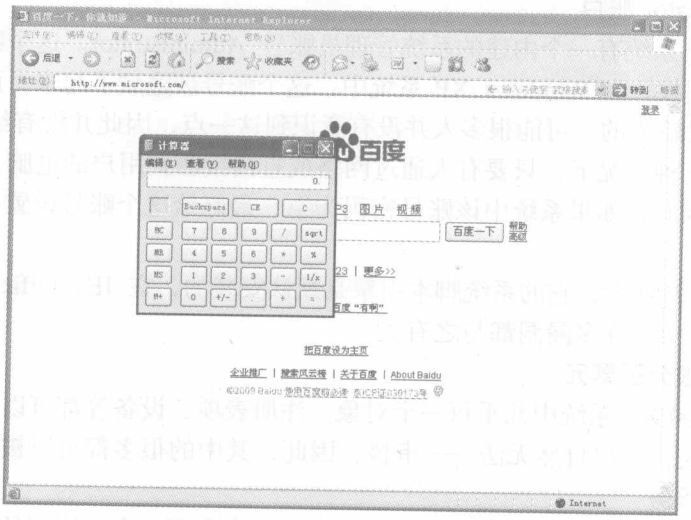


图 1-5 打开系统自带的计算器

如果 IE 浏览器没有“http：//”自动补充功能，则可启动快捷方式所指向的可执行文件。虽然微软公司已经声明该 Bug 并非安全隐患，只是 Windows 操作系统和 IE 浏览器的功能特性，类似的操作完全属于合理行为。但该 Bug 还是很容易被攻击者利用，以执行一些特

殊代码，而且不会受到 Windows 系统本身的阻挠。

1.2 Windows 操作系统中的漏洞

由于硬件原因和各种主客观因素的影响，使 Windows 操作系统中存在了一些漏洞。这些漏洞如果被别有用心的人利用，则会给用户的系统安全带来一定危险。

1.2.1 Windows 系统漏洞简介

漏洞是硬件、软件、协议的具体实现，或系统安全策略上存在的缺陷，可以使攻击者在未授权的情况下访问或破坏系统。漏洞影响到的范围非常大，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换言之，在不同的软、硬件设备中都可能存在安全漏洞，在不同种类的软硬件设备之间，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都存在不同的安全漏洞。

Windows 系统漏洞是特指 Windows 操作系统在逻辑设计上的缺陷，或在编写时产生的错误，这个缺陷或错误可以被不法者或电脑黑客利用，通过植入木马、病毒等方式来攻击或控制整个电脑，从而窃取电脑中的重要资料和信息，甚至破坏系统。

Windows 系统漏洞问题是与时间紧密相关的。一个 Windows 系统从发布的那一天起，随着用户的深入使用，系统中存在的漏洞将会被不断暴露出来，这些早先被发现的漏洞也会不断被系统供应商（微软公司）发布的补丁软件修补，或在以后发布的新版系统中得以纠正。而在新版系统纠正了旧版本中漏洞的同时，也会引入一些新的漏洞和错误。例如，目前比较流行的是 ani 鼠标漏洞，即是由于利用了 Windows 系统对鼠标图标处理的缺陷，木马作者制造畸形图标文件从而溢出，木马就可以在用户毫不知情的情况下执行恶意代码。

因此，随着时间的推移，旧的系统漏洞将会不断消失，新的系统漏洞也会不断出现，系统漏洞问题也会长期存在。

1.2.2 Windows 9x 中的漏洞

Windows 9x 操作系统中存在着大量的漏洞，其中有些比较典型，对今天的学习和应用仍然有相当大的参考和借鉴意义。

1. IGMP 漏洞

漏洞描述：IGMP（Internet Group Management Protocol，互联网组管理协议）漏洞是一个较有名且危险的系统漏洞，可使用户计算机中断网络连接或出现蓝屏和死机。

解释：目前有很多可发动 IGMP 攻击的工具，如 Winnuke、Sping 和 Tardrop 等。通过这些工具可向某个 IP 地址的 100 端口，不断发送大量的 IGMP 数据包，当被攻击的计算机收到数据包后，无法对数据进行处理，从而导致 TCP/IP 崩溃，引起系统中断网络连接或出现蓝屏现象，此时重启系统才可解决该问题。此外，如果攻击者进行端口监听，还可对其他端口进行攻击。

对策：

1）下载相关的补丁程序，网址如下。

Windows 98 第 1 版：http://www.virusview.net/download/patch/oob/up98igmp.zip