黑客技术典型应用系列

200分钟
DVD多媒体
讲解视频

黑客防范技巧与典型应用

武新华　段玲华　刘　岩　等编著

- 有效抵抗与主动防御双管齐下，知己知彼，打造固若金汤的入侵防范系统。
- 通过典型实例全面解析黑客防范技巧，工具软件、应用环境和实战经验尽在其中。
- 网络安全高手点拨技术难点，多媒体视频直观再现实战场景，全力弥补读者知识断层。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客技术典型应用系列

黑客防范技巧与典型应用

武新华　段玲华　刘　岩　等编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书紧紧围绕黑客防范技巧及其典型应用，针对用户在进行黑客防御时要用到的技术进行“傻瓜式”的讲解，以使读者对网络防御技术形成系统的了解，能够更有效地防范黑客的攻击。全书共分为 11 章，主要内容包括 Windows 系统漏洞防范、木马与间谍软件的伪装与查杀、浏览器恶意攻击和防御、QQ 的攻击与防御技术、电子邮件防御实战、后门与自身防护技术、网络代理与恶意进程清除、远程控制工具与防御、备份升级与数据恢复、病毒木马主动防御清除、打好网络安全防御战等。

本书内容丰富、图文并茂、深入浅出，适合广大网络爱好者阅读，也适合网络安全从业人员及网络管理员参考。

图书在版编目（CIP）数据

黑客防范技巧与典型应用/武新华等编著. —北京：中国铁道出版社，2009.5
（黑客技术典型应用系列）
ISBN 978-7-113-10017-9

Ⅰ.黑… 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 072839 号

书　　名：黑客防范技巧与典型应用
作　　者：武新华　段玲华　刘岩　等编著

策划编辑：严晓舟　荆　波
责任编辑：苏　茜　　**编辑部电话：**（010）63583215
编辑助理：吴春英　　**封面制作：**白　雪
封面设计：付　巍
责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：北京鑫正大印刷有限公司
版　　次：2009 年 7 月第 1 版　　2009 年 7 月第 1 次印刷
开　　本：787mm×1092mm　1/16　　**印张：**24.25　　**字数：**570 千
印　　数：4 000 册
书　　号：ISBN 978-7-113-10017-9/TP・3289
定　　价：45.00 元（附赠光盘）

前　言

随着全球信息化的高速发展、互联网的日益普及和信息化工程的快速建设，电子商务、电子政务、网上银行、网络游戏等，已成为当前 IT 技术的应用热点。社会各方面对网络和信息技术的依赖程度不断增强，网络已逐渐成为人们工作和生活中必不可少的一部分。网络在给人们带来极大便利的同时，黑客入侵和网络安全也同样给人们的工作和生活带来了不利的影响，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、木马产业链等的严重危害，更使得网络安全问题成为大家关注的焦点。

由于互联网本身存在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，其影响已通过互联网逐步扩大到政府、通信、广电、金融、电力、交通等领域，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。

因此，必须采取有力措施加强网络自身安全的防护性能，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、多样化的攻击和破坏活动的频繁发生，攻击点也越来越趋于精确和集中，攻击破坏的影响面不断扩大并产生连环效应，因此必须构筑一种主动的安全防御系统，才有可能最大限度地有效应对黑客攻击方式的各种变化。

本书的写作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和主动防御的方法与关键技术，提高用户安全防护意识。本书是一本实用的网络安全工具书，适用于网络信息安全专业的技术人员、网络安全管理人员、网络使用者及信息时代的创业者阅读。

此外，本书还从黑客入侵防护应用角度给出了相对独立的论述，使读者对如何建构一个实用的黑客入侵防范体系有一个基本概念和思路，并为读者提供了几种典型的安全防护系统建设方案，供读者参考和借鉴。

本书特色如下：

- 通俗易懂，由浅入深，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。
- 注重实用性，理论和实例相结合，并配以插图和配套光盘视频讲解，力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门，提高读者的效率，并节省读者宝贵的时间。
- 重点突出、操作简练、内容丰富，同时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。

作者采用任务驱动的方式讲解，揭秘每一种黑客攻击的手法；披露黑客常用的攻击技术，让您知己知彼，掌握攻防互参的防御方法，全面确保您的网络安全。

本书由武新华、段玲华、刘岩等编著。其中，武新华负责第 1 章，李防负责第 2 章，李秋菊负责第 3 章，陈艳艳负责第 4 章，杨平负责第 5 章，段玲华负责第 6 章和第 11 章，张克歌负

责第 7 章，刘岩负责第 8 章，王英英负责第 9 章，孙世宁负责第 10 章，最后由武新华通审全稿。本书在编写过程中得到了许多热心网友的支持，参考了大量同类的书籍与资料，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。

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。

编　者

2009 年 3 月

郑重声明：

本书目的绝不是为那些怀有不良动机的人提供技术支持，也不承担因为技术被滥用所产生的连带责任；希望读者在阅读本书后，不要使用书中所讲技术进行任何违法行为，否则后果自负，切记切记！

目　录

第 1 章　Windows 系统漏洞防范

本章精粹

通过学习本章，可以使读者掌握如何为系统打补丁的技巧，解密黑客任意篡改他人计算机系统的伎俩，并更加全面地掌握组策略和注册表方面的知识，为黑客防御措施奠定坚实的知识基础。

重点提示

- 设置组策略实现安全登录
- 注册表编辑器实用防范
- Windows 系统的密码保护
- Windows 系统的安全设置

随着互联网的普及和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，且 Windows 操作系统本身具有的漏洞，为黑客的入侵行为提供了便利之门。所谓“知己知彼，百战不殆”，要想全面防止黑客的入侵，首先就需要了解黑客是怎样发现漏洞并对漏洞进行攻击的。

1.1　设置组策略实现安全登录

在计算机的具体应用过程中，为实现某些正常的操作，管理员需要为用户和计算机定义并控制程序、网络资源及操作系统的行为等，而实现这些操作的工具就是组策略，所以要想安全地登录计算机，必须设置好组策略。

1.1.1　组策略概述

在介绍组策略之前，应该先了解注册表，注册表是 Windows 系统中保存系统软件和应用软件配置的数据库。随着 Windows 系统功能的逐渐丰富，注册表中的配置项目越来越多。很多配置都可以自定义设置，但这些配置分布在注册表的各个角落，如果是手工配置，就显得尤为困难和烦杂。而组策略则将系统重要的配置功能汇集成各种配置模块，供用户直接使用，从而达到方便管理计算机的目的。

简单地说，组策略设置就是修改注册表中的配置。当然，组策略使用了更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

1．组策略的版本

组策略是 Windows 9x/NT 中系统策略的高级扩展，具有更多的管理模板、更灵活的设置对

象及更多功能，目前主要应用在 Windows 2000/XP/2003 系统中。

系统策略编辑器支持对当前注册表的修改，也支持连接到网络中的计算机并对其注册表进行设置。而组策略及其工具可对当前注册表进行直接修改。组策略工具还可以打开网络上的计算机并进行配置，甚至可以打开某个 Active Directory 对象（即站点、域或组织单位）并对其进行设置。无论是系统策略还是组策略，其基本原理都是修改注册表中相应的配置项目，从而达到配置计算机的目的，只是其中的一些运行机制发生了变化和扩展而已。

2．运行组策略

运行组策略实现某些控制操作的具体操作步骤如下：

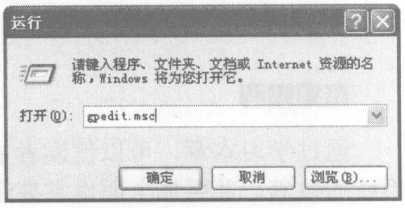

图 1-1　“运行”对话框

步骤 1 由于 Windows 2000/XP/2003 系统中系统已默认安装了组策略，这里无须安装，选择“开始”→“运行”命令，打开“运行”对话框，如图 1-1 所示。

步骤 2 在“打开”文本框中输入 gpedit.msc 命令，单击“确定”按钮，进入“组策略”窗口，如图 1-2 所示。

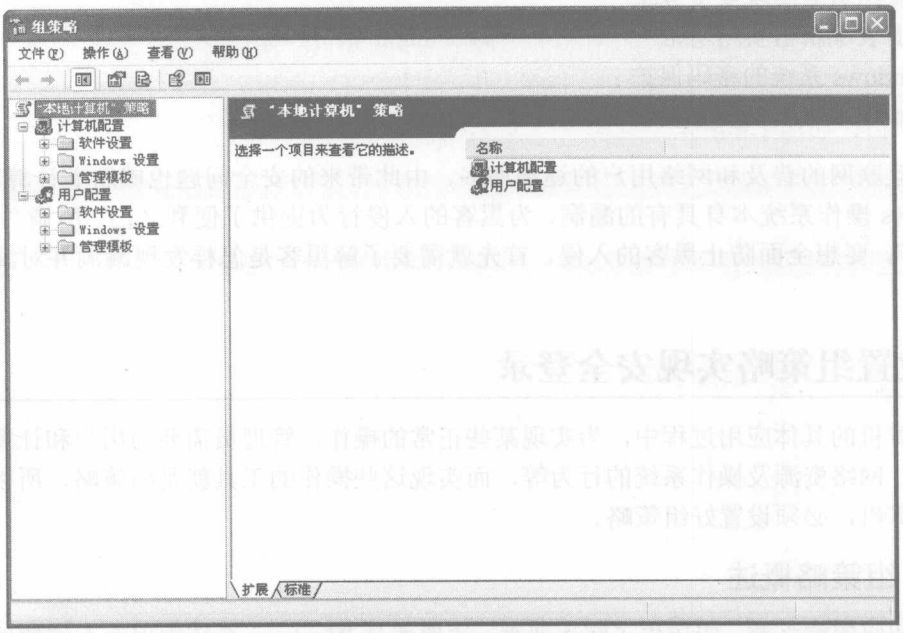

图 1-2　“组策略”窗口

步骤 3 该窗口中显示的组策略是当前计算机，在其中选择要更改的选项之后，选择“用户配置”→“管理模板”→“任务栏和「开始」菜单”选项，打开“任务栏和「开始」菜单”窗口，如图 1-3 所示。

步骤 4 右击“关闭通知区域清理”选项，从弹出的快捷菜单中选择“属性”命令，打开“关闭通知区域清理属性”对话框，根据实际需要选择相应的单选按钮对计算机策略进行管理，如图 1-4 所示。

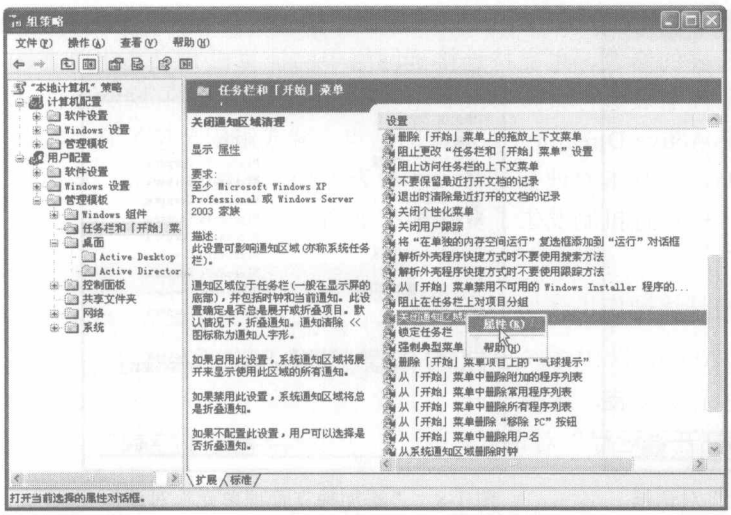

图 1-3　"任务栏和「开始」菜单"窗口

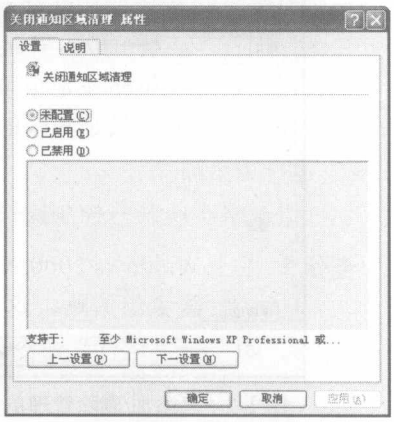

图 1-4　"关闭通知区域清理属性"对话框

步骤 5 如果需要配置其他计算机策略，则选择"开始"→"运行"命令，在"运行"对话框中输入 mmc 命令，如图 1-5 所示。单击"确定"按钮，进入"控制台 1"窗口，如图 1-6 所示。

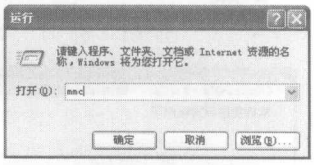

图 1-5　输入 mmc 命令

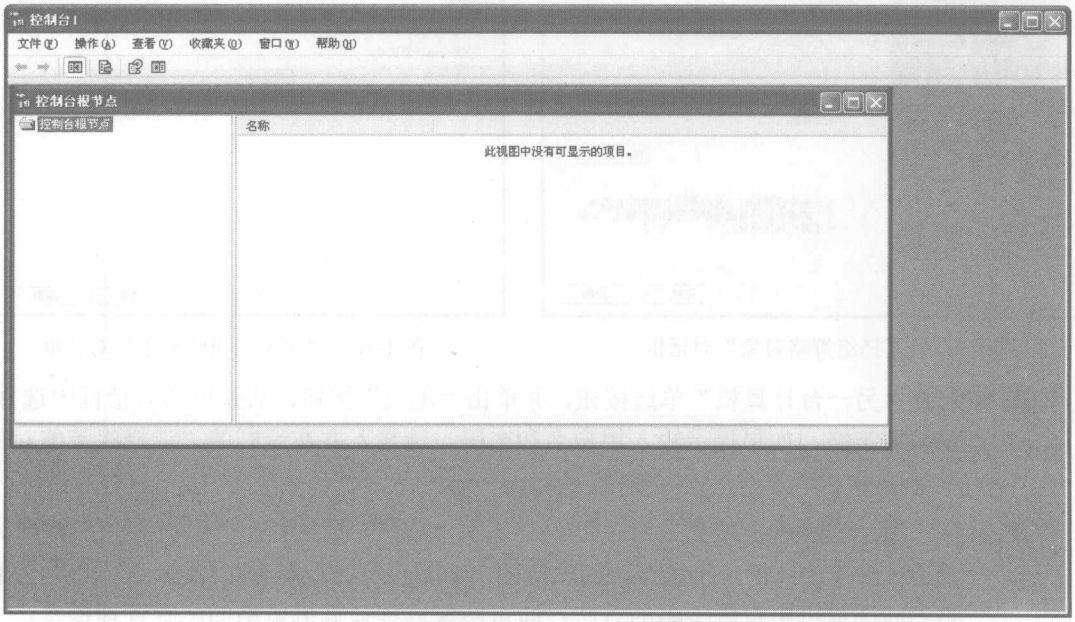

图 1-6　"控制台 1"窗口

步骤 6 选择"文件"→"添加/删除管理单元"命令，打开"添加/删除管理单元"对话框，如图 1-7 所示。单击"添加"按钮，打开"添加独立管理单元"对话框，选择"组策略对象编辑器"选项，如图 1-8 所示。

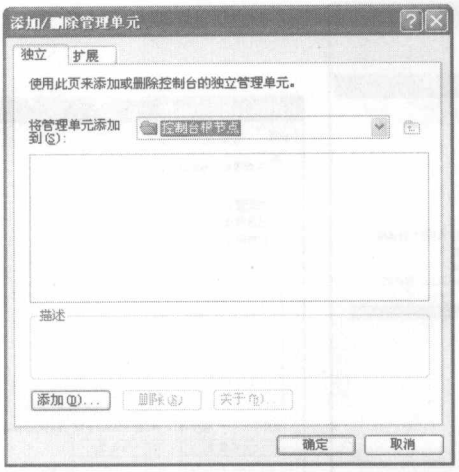

图 1-7 “添加/删除管理单元”对话框

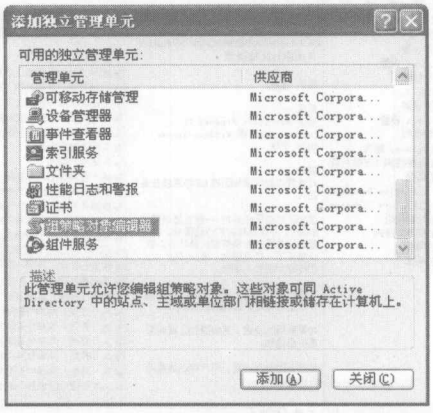

图 1-8 “添加独立管理单元”对话框

步骤 7 单击“添加”按钮，打开“选择组策略对象”对话框，如图 1-9 所示。单击“浏览”按钮，打开“浏览组策略对象”对话框，如图 1-10 所示。

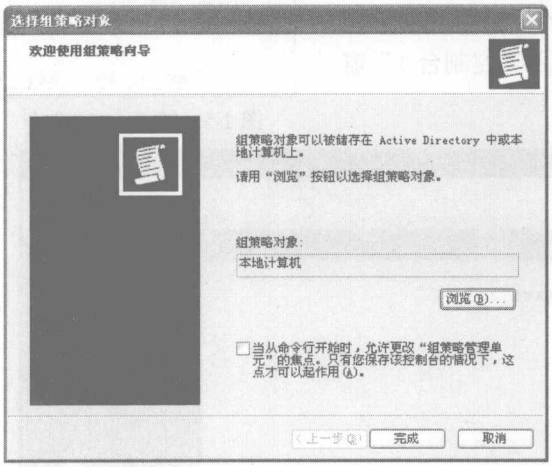

图 1-9 “选择组策略对象”对话框

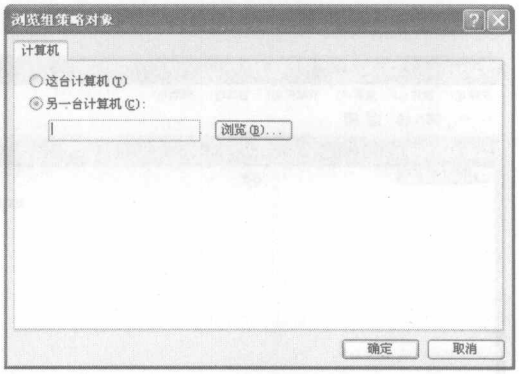

图 1-10 “浏览组策略对象”对话框

步骤 8 选择“另一台计算机”单选按钮，并单击“浏览”按钮，从弹出的对话框中选择需要的组策略，如果提示输入用户名和密码，请输入并在返回的“选择组策略对象”对话框中，单击“完成”按钮。

步骤 9 在“添加独立管理单元”对话框中，单击“关闭”按钮并在“添加/删除管理单元”对话框中单击“确定”按钮，则选定的 GPO 显示在控制台根结点下。此时，再按照当前计算机中设置策略的方法，即可实现远程计算机策略的配置管理操作。

3. 管理组策略中的管理模板

默认情况下，在 Windows 2000/XP/2003 系统中包含有几个 ADM 文本文件，这些文本文件被称为管理模板，并为“管理模板”文件夹下的项目提供策略信息。默认的 Admin.adm 管理模板位于系统文件夹的 INF 文件夹中，同时包含了默认安装下的 4 个模板文件，具体体现在：

- System.adm：默认安装在组策略中，用于设置系统。
- Inetres.adm：默认安装在组策略中，用于 Internet Explorer 策略设置。
- Wmplayer.adm：用于 Windows Media Player 设置。
- Conf.adm：用于 NetMeeting 设置。

组策略中有多个管理模板可供使用，用户如果要使用新模板，可通过添加操作来实现。具体操作步骤如下：

步骤 1 在“组策略”窗口中可添加“计算机配置”和“用户配置”模板，如果要添加“用户配置模板”，可右击“用户配置”下的“管理模板”选项，从弹出的快捷菜单中选择“添加/删除模板”命令，打开“添加/删除模板”对话框，如图 1-11 所示。

步骤 2 单击“添加”按钮，打开“策略模板”对话框，如图 1-12 所示。选择要添加的模板文件，单击“打开”按钮，完成添加操作，如图 1-13 所示。

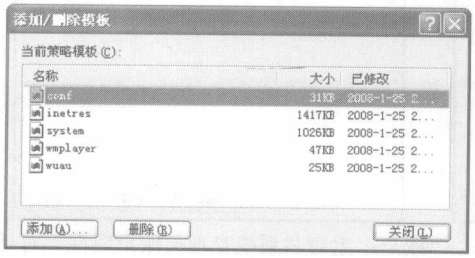

图 1-11　“添加/删除模板”对话框

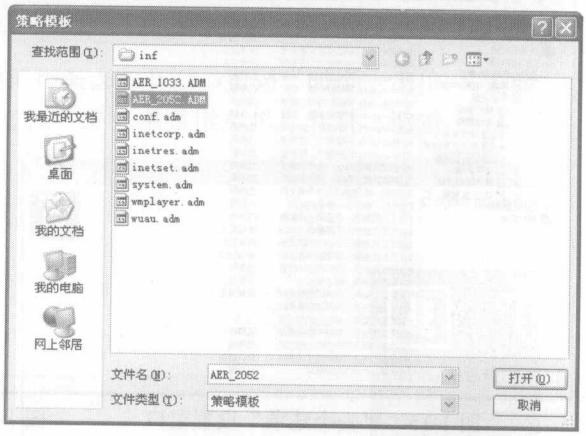

图 1-12　“策略模板”对话框

步骤 3 单击“关闭”按钮返回到“组策略”窗口中，选择“用户配置”→“管理模板”选项并单击相应目录树，即可看到新添加的管理模板所产生的配置项目，如图 1-14 所示。

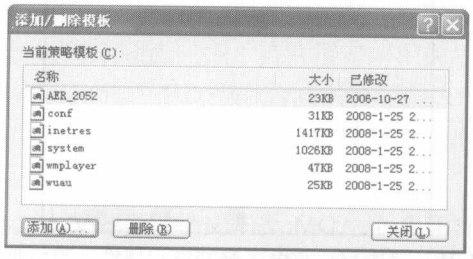

图 1-13　添加策略模板

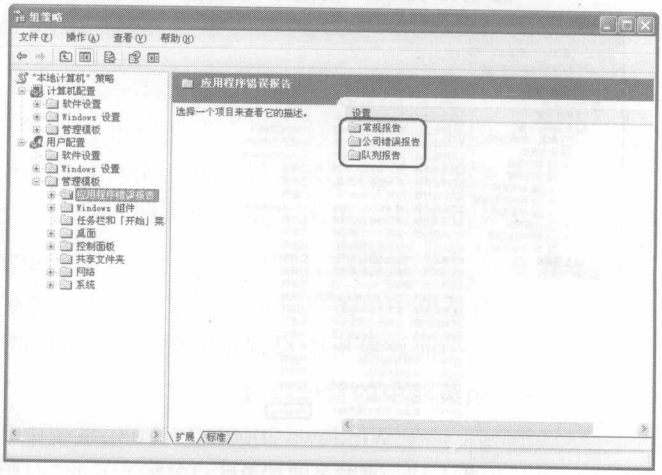

图 1-14　添加配置项目显示