中国科学出版集团
新世纪书局

黑客高手
完全揭密

最新攻击和防御技巧

最新
黑客攻防实战
从入门到精通 第2版

武新华 孙振辉 编著

教你如何防范

- 服务器被侵入
- 局域网被攻击
- 银行账号被破解
- 敏感资料被窃取

1DVD
情境式多媒体语音教学光盘

- 300分钟32个任务的多媒体语音教学课程
- 本书PPT电子课件

★ 专业经验分享
作者团队由具有十余年网络安全和教学经验的专家组成，其编写的图书在业界有深远的影响

★ 攻防实战训练
提供大量操作实例，任务驱动式教学，让你在边学边练中快速提高实战技能

★ 全程技术服务
专业答疑网站：
www.newtop01.com
在线技术支持QQ：274648972

科学出版社

最新

黑客攻防实战

从入门到精通 第2版

武新华 孙振辉 编著

科学出版社

内 容 简 介

全书对每一个入侵步骤作详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答。全书共分为14章，内容主要包括：管理员账户攻防策略、局域网攻击实例演示、漏洞溢出入侵与防范、远程控制的攻击与防范、QQ邮箱账号攻防策略、间谍软件的清除和系统清理、木马入侵与清除技术、从口令破解到隐藏账户后门、黑客常用入侵工具使用、网络欺骗与入侵技术、入侵检测和蜜罐技术、黑客防范实战演练、代理与日志清除技术、网络攻击案例演示等内容。

本书内容丰富，图文并茂，深入浅出，面向广大网络爱好者，可作为一本速查手册，也适用于网络安全从业人员及网络管理者。

图书在版编目（CIP）数据

最新黑客攻防实战从入门到精通/武新华，孙振辉编著. —2版. —北京：科学出版社，2010

ISBN 978-7-03-029600-9

I. ①最… II. ①武…②孙… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆CIP数据核字（2010）第228421号

责任编辑：王海霞 赵东升 / 责任校对：杨慧芳

责任印刷：新世纪书局 / 封面设计：周智博

科学出版社出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

中国科学出版集团新世纪书局策划

北京市鑫山源印刷有限公司

中国科学出版集团新世纪书局发行 各地新华书店经销

*

2011年2月 第 二 版 开本：16开

2011年2月第一次印刷 印张：29.75

印数：1—3 000 字数：724 000

定价：58.00元（含1DVD价格）

（如有印装质量问题，我社负责调换）

前　言

您知道在每天上网时，有多少黑客正在浏览您计算机中的重要数据吗？黑客工具的肆意传播，使得即使是稍有点计算机基础的人，就可以使用简单的工具对网络中一些疏于防范的主机进行攻击，在入侵成功之后，对其中的数据信息为所欲为。当用户发现密码被盗、资料被修改或删除、硬盘变作一团空白时，再想亡羊补牢，却为时已晚。

本书内容

为了使读者在最短的时间内轻松掌握电脑各方面应用的基本知识，快速解决实际生活中遇到的问题，特意为广大读者朋友量身定制了这本《最新黑客攻防实战从入门到精通（第2版）》。本书作为指导初学者快速掌握黑客攻防知识的入门书籍，打破了传统的按部就班的讲解模式，以解决问题为出发点，通过大量来源于实际的精彩实例，全面涵盖了读者在防御黑客攻击的过程中所遇到的问题并提供解决方案。

本书以配图、图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，注重对操作技巧的剖析，不但介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，而且详细地讲述了防范黑客攻击的方法，使读者在了解基本网络安全知识的前提下，轻松而快速地掌握基本的反黑知识、工具和修复技巧，在遇到别有用心者的入侵时能够不再茫然无措。

增值服务

本书配套 DVD 光盘提供了多种攻防实战的教学视频，汇集了众多高手的操作精华，通过提高读者对主流操作手法的感性认识，使读者的学习更高效。

此外，如发现本书中有不妥或需要改进之处，还可通过访问 http://www.newtop01.com 或 QQ：274648972 与笔者进行沟通，笔者将衷心感谢提供建议的读者，并真心希望在和广大读者互动的过程中能得到提高，在此致谢，谢谢！

本书特色

本书紧紧围绕“攻”、“防”两个不同的角度，在讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网络入侵与防御的全过程。

- 真正以图来解释每一个知识点及操作实例，基础知识讲解、范例与练习结合，学习周期最短，阅读最轻松。
- 作者采用最为通俗易懂的图文解说，“理论+实战 图文+视频=全面提升学习效率”，即使是电脑新手也能通读全书。
- 以任务驱动、情景教学的方式来介绍，在学习案例的过程中掌握知识点，学习目的性、指向性最强。最新黑客技术盘点，让读者实现“先下手为强”。

读者对象

本书作为一本面向广大网络爱好者的速查手册，适合如下读者学习使用：

- 电脑爱好者、提高者。
- 具备一定黑客知识基础和工具使用基础的读者。
- 网络管理人员。
- 喜欢研究黑客技术的网友。
- 大中专院校相关专业的学生。

本书作者

本书作者团队长期从事网络安全管理工作，都具有较强的实践操作能力及一线拼杀经验，可带领广大醉心技术者穿越迷雾，把黑客们的伎俩看清楚。本书的编写情况是：娄志刚负责第 1 章，孙晓红负责第 2 章，崔江红负责第 3 章，李防负责第 4 章，陈旭生负责第 5 章，高旻睿负责第 6 章，段夕红负责第 7 章，孙世宁负责第 8 章，贺鹏负责第 9 章，郭毓负责第 10 章，姜昭一负责第 11 章，华敏负责第 12 章，李杰负责第 13 章，王红负责第 14 章，最后由武新华通审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有失误、遗漏之处，因此，还望大家以宽容为本，慈悲为怀，本着共同探讨、共同进步的平和心态来阅读本书。作者心存谨敬，随时恭候您提出的宝贵意见。

最后，需要提醒大家的是：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介绍的黑客技术对别人进行攻击，否则后果自负，切记切记!

编 者

2010 年 11 月

目　录

管理员账户攻防策略

本章主要以 Windows 系统为例讲述管理员账号的攻防策略，Windows 管理员账号是最基本的保护计算机资源的方法，但不足以抵挡高级黑客的入侵。本章内容有助于读者全面认识管理员账号存在的一些安全隐患。

学习要点

- 破解管理员账户
- 设置管理密码保障账户安全
- 禁用 Guest 账户保障系统安全
- 禁用共享资源保障系统安全

Windows XP 的风靡引来了无数黑客的注意，进而出现了层出不穷的攻击手段，黑客究竟是如何攻破管理员账号的？又该如何针对这些攻击手段做好防范工作呢？

1.1 破解管理员账户

在 Windows XP 中提供了管理员账号功能，用户可以通过创建管理员账户并设置密码，来防止其他人进入自己的计算机随意浏览系统资源。但是，黑客可以在不知道管理员密码的情况下，使用多种攻击手段破解管理员的账户及密码，计算机资源被黑客一览无余。

1.1.1 使用 Administrator 账户登录

通常情况下，用户都习惯在系统中创建一个容易记忆的管理员账号及密码，以方便自己登录系统。其实在 Windows 系统安装完毕之后，会自动创建一个账号为 Administrator 的超级管理员账户，且密码默认为空。这个超级管理员账户很容易被用户忽略，如果没有设置该账号的密码，就会成为黑客攻击的一个安全隐患。

下面通过实例讲述如何利用不设置密码的 Administrator 账户登录用户计算机，具体操作步骤如下。

01 按下机箱开机电源，即可启动计算机。当用户创建了账号及密码，在进入 Windows 登录界面时会出现如图 1–1 所示的画面。此时，在白色输入框中输入正确的密码即可进入系统。

02 按 Ctrl+Alt+Delete 组合键，即可打开【登录到 Windows】对话框，在【用户名】文本框中显示的是用户账号，如图 1–2 所示。

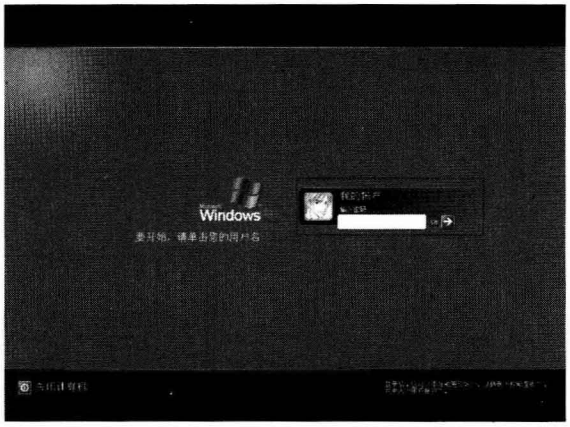

图 1-1 Windows 登录界面

图 1-2 【登录到 Windows】对话框

03 将原有的用户账号删除，在【用户名】文本框中输入 Administrator，如图 1–3 所示。单击【确定】按钮，即可进入系统界面。

此时，黑客只是通过 Administrator 账号进入用户计算机。不仅如此，黑客还可以通过 Administrator 账户的权限删除和更改用户账号，具体的操作步骤如下。

01 在使用 Administrator 账号成功登录系统之后，选择【开始】→【控制面板】菜单项，即可打开【控制面板】窗口，如图 1–4 所示。

图 1-3　输入 Administrator

图 1-4　【控制面板】窗口

02 双击【控制面板】窗口中的【用户账户】图标，即可打开【用户账户】窗口，如图 1–5 所示。此时，单击【我的账户】选项，即可打开【您想更改 我的账户的账户的什么】界面，如图 1–6 所示。

图 1-5　【用户账户】窗口

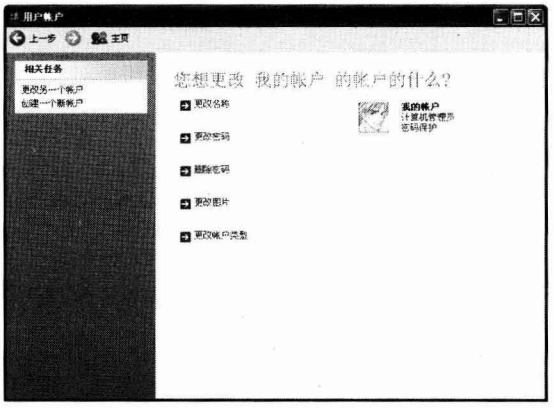

图 1-6　【您想更改 我的账户 的账户的什么】界面

03 此时，如果黑客想要将该用户账户的密码清空，则单击【删除密码】超链接，即可进入【您确实要删除 我的账户 的密码吗】界面，如图 1–7 所示。单击【删除密码】按钮，即可清除该用户账户的登录密码，重启计算机后，即可不使用密码以该用户账户身份登录系统。

04 若黑客想要为该用户账号添加一个新的密码，让用户无法以之前的账号正常登录系统，只须返回【您想更改 我的账户 的账户的什么】界面，单击【更改密码】超链接，即可进入【为 我的账户 的账户创建一个密码】界面，分别在【输入一个新密码】和【再次输入密码以确认】文本框中输入新的登录密码，如图 1–8 所示。

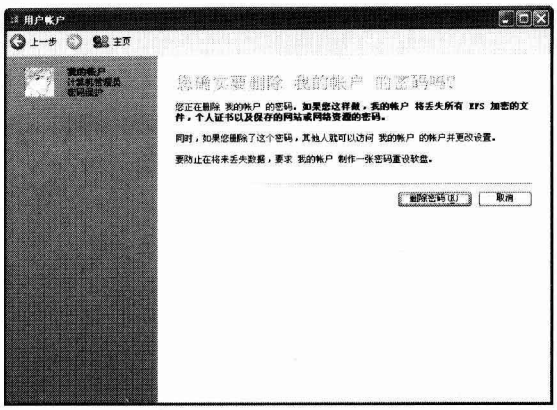

图 1-7 【您确实要删除 我的账户 的密码吗】界面

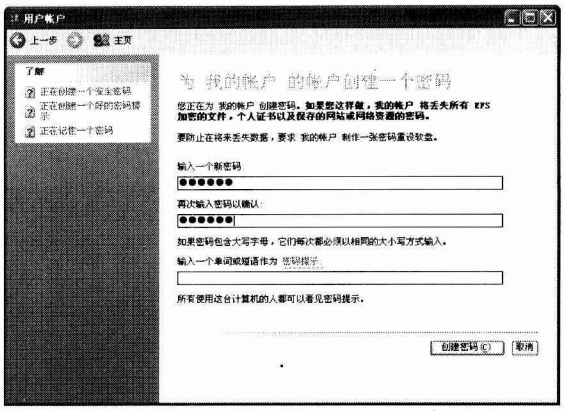

图 1-8 【为 我的账户 的账户创建一个密码】窗口

05 单击【创建密码】按钮，即可完成对该用户账户登录密码的创建。

1.1.2 使用 Password Changer 软件强制清除管理员密码

设置 Administrator 账户及用户账户密码虽然可以提高系统的安全性，但也不是绝对安全，黑客同样可以使用第三方软件对这些账号的密码进行清除，如常见的 Password Changer 软件。Password Changer 软件是一款基于 DOS 的系统密码重置工具，设计者的本意是为了在管理员密码丢失的情况下，方便用户对指定账户的登录密码清除重置。而在黑客手中却被用来破解系统密码，以达到盗窃用户计算机信息的目的。

（1）安装 Password Changer 软件

01 双击下载的 Password Changer Demo Setup.exe 应用程序，即可打开 Active@ Password Changer Demo 对话框，如图 1-9 所示。

02 单击 Next 按钮，即可打开 Licensing Policy 界面，在其中选择 I Agree to the terms of the license 单选按钮，如图 1-10 所示。

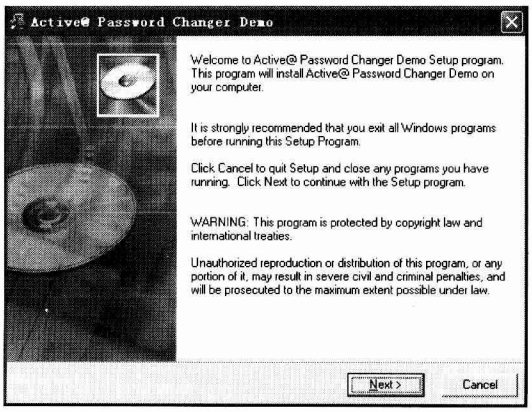

图 1-9 Active@ Password Changer Demo 对话框

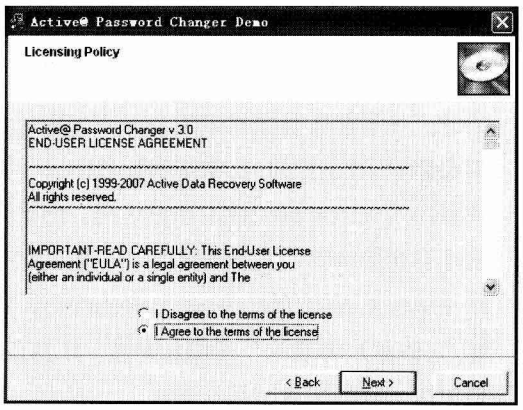

图 1-10 Licensing Policy 界面

03 单击 Next 按钮，即可打开 Destination Location 界面，单击 Browse 按钮可更改安装路径，如图