

<<电脑黑客攻防技巧>>

图书基本信息

书名：<<电脑黑客攻防技巧>>

13位ISBN编号：9787121149986

10位ISBN编号：7121149982

出版时间：2012-1

出版时间：电子工业出版社

作者：先知文化

页数：287

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<电脑黑客攻防技巧>>

内容概要

本书以技巧的形式详细解读了黑客攻击与防范的相关知识，主要内容包括：黑客基础知识、黑客常用命令与工具、Windows系统安全防范、信息收集与漏洞扫描、密码攻防、远程控制攻防、网络攻防、QQ和E-mail攻防、木马攻防、防范电脑病毒以及防范间谍软件与流氓软件等知识。本书在内容的安排上简化了理论知识的介绍，突出实际操作，并精选了大量实用的操作技巧和经验，以条目形式进行编排，方便查询和阅读。本书不仅适合喜爱黑客知识的初学者，更适合所有关心电脑及个人信息安全的用户。

本书的作用在于让读者能够对黑客知己知彼，从而保证个人电脑及信息安全，切勿使用黑客技术对他人电脑进行攻击。

<<电脑黑客攻防技巧>>

书籍目录

第1章 黑客基础知识

1.1 认识黑客

技巧1 什么是黑客

技巧2 黑客常用的攻击手段

1.2 IP地址与端口

技巧1 认识IP与IP地址

技巧2 认识端口及其分类

技巧3 查看端口

技巧4 关闭端口

技巧5 限制端口

1.3 熟悉系统进程

技巧1 查看系统中运行的进程

技巧2 怎样查看进程起始位置

技巧3 如何查看他人电脑中的系统进程

技巧4 如何判断系统进程是否正常

技巧5 关闭正在运行的进程

技巧6 新建系统进程

技巧7 查看隐藏的进程

技巧8 如何查杀病毒进程

第2章 黑客常用的命令与工具

2.1 基本DOS命令

技巧1 使用dir命令显示目录

技巧2 使用cd命令进入目录

技巧3 使用rd命令删除目录

技巧4 使用md命令新建目录

技巧5 使用del命令删除文件

技巧6 在DOS环境下常用的快捷键

2.2 网络命令应用

技巧1 使用ping命令测试网络

技巧2 使用net命令管理网络

技巧3 使用ftp命令上传下载文件

技巧4 使用telnet命令登录远程电脑

技巧5 使用at命令执行任务

技巧6 使用netstat命令显示网络连接信息

技巧7 使用arp命令显示与修改本地ARP信息

技巧8 使用systeminfo命令显示系统信息

技巧9 使用nslookup命令诊断域名系统

技巧10 使用ipconfig命令查看网络配置信息

2.3 黑客常用工具

技巧1 使用HostScan扫描网络主机

<<电脑黑客攻防技巧>>

技巧2 使用流光扫描器

技巧3 使用网络神偷远程控制器

技巧4 使用SSS扫描器

技巧5 其他黑客常用软件

第3章 Windows系统安全

防范

3.1 修补系统漏洞

技巧1 了解系统漏洞

技巧2 利用系统更新及时修复系统漏洞

技巧3 使用金山卫士修复系统漏洞

技巧4 使用360安全卫士修复系统漏洞

3.2 系统安全设置

技巧1 禁用来宾账户

技巧2 防止ping命令探测系统

技巧3 设置代理服务器隐藏IP

技巧4 查看默认共享

技巧5 关闭默认共享

技巧6 当用户离开时快速锁定桌面

3.3 注册表安全设置

技巧1 熟悉注册表

技巧2 禁止远程修改注册表

技巧3 禁止其他用户在桌面上添加

快捷方式

技巧4 禁止危险的启动项

技巧5 永久关闭默认共享

技巧6 禁止普通用户查看事件记录

技巧7 揪出隐藏的超级用户

技巧8 设置注册隐藏“开始”菜单的

快捷命令

技巧9 配置注册表防止DDoS攻击

技巧10 禁止播放网页中的动画、声音

和视频

技巧11 发生错误时不弹出警告窗口

3.4 组策略安全设置

技巧1 熟悉组策略

技巧2 设置账户锁定策略

技巧3 禁用重要策略选项

技巧4 禁止远程访问注册表

技巧5 使用批处理文件在每次启动

系统时关闭默认共享

技巧6 禁止更改桌面设置

技巧7 禁用“开始”菜单中的命令

技巧8 禁止访问控制面板

技巧9 关闭135端口

技巧10 利用组策略锁定注册表

技巧11 利用组策略清理上网痕迹

技巧12 利用组策略启用重要系统功能

<<电脑黑客攻防技巧>>

技巧13 只有本地登录的用户才能访问
CD-ROM

第4章 信息搜集与漏洞扫描

4.1 搜集信息

技巧1 使用ping命令获取IP地址

技巧2 使用专业网站获取IP地址

技巧3 使用超级IP查询工具获取目标
物理位置

技巧4 通过专业网站查询IP地址
所在位置

技巧5 查询网站备案信息

4.2 检测系统漏洞

技巧1 使用漏洞扫描器检查系统漏洞

技巧2 使用X-Scan扫描器检查系统
漏洞

技巧3 使用MBSA检测系统安全性

技巧4 使用瑞星系统安全漏洞扫描检测
系统漏洞

技巧5 使用系统漏洞扫描助手扫描系统
漏洞

4.3 扫描服务和端口

技巧1 使用SuperScan扫描器扫描服务
和端口

技巧2 使用LanSee局域网查看工具查看
他人主机中的端口

技巧3 使用黑客字典编辑弱口令的
扫描规则

技巧4 使用弱口令扫描器获取口令

技巧5 使用Nmap扫描器

技巧6 解决使用扫描工具过程中出现
突然停止响应的现象

技巧7 解答使用端口扫描器时扫描
不到QQ程序开放端口的原因

第5章 密码攻防

5.1 BIOS密码攻防

技巧1 设置BIOS用户密码

技巧2 设置BIOS超级用户密码

技巧3 设置密码检测方式

技巧4 利用CMOS放电法破解BIOS密码

技巧5 利用跳线短接破解BIOS密码

5.2 操作系统密码攻防

技巧1 设置账户登录密码

技巧2 设置电源管理密码

技巧3 设置屏幕保护密码

技巧4 利用密码重设盘破解系统密码

技巧5 利用软件破解系统管理员密码

技巧6 删除Sam文件破解Windows

<<电脑黑客攻防技巧>>

登录密码

技巧7 破解Windows屏保密码

5.3 办公文档密码攻防

技巧1 加密Word文档

技巧2 设置窗体保护

技巧3 加密Excel文档

技巧4 查看Access数据库密码

技巧5 破解Office文档密码

技巧6 利用WinRAR加密文件

技巧7 破解RAR压缩文件密码

技巧8 破解ZIP文件密码

技巧9 破解Outlook Express密码

技巧10 破解PDF文档密码

技巧11 破解Foxmail账户密码

技巧12 查看星号“*”密码

技巧13 破解使用Windows优化大师

加密的文件

第6章 远程控制攻防

6.1 Windows 7远程桌面连接

技巧1 允许远程桌面连接

技巧2 发起远程桌面连接

技巧3 向远程桌面传送文件

6.2 Windows 7远程协助

技巧1 允许远程协助

技巧2 邀请他人远程协助

技巧3 利用远程协助帮助他人

技巧4 远程协助和远程桌面的区别

6.3 使用工具实现远程控制

技巧1 使用腾讯QQ实现远程控制

技巧2 使用QQ远程控制获取被控端

主机文件

技巧3 使用QQ远程控制关闭被控端主机

技巧4 使用QuickIP实现远程控制

技巧5 使用pcAnywhere实现远程控制

技巧6 使用灰鸽子实现远程控制

第7章 网页攻防

7.1 查杀与防范网页恶意代码

技巧1 什么是网页恶意代码

技巧2 恶意代码的传播方式和趋势

技巧3 网页恶意代码的攻击原理与方式

技巧4 查杀网页恶意代码

技巧5 防范网页恶意代码

技巧6 解决主页设置锁定的问题

7.2 网络炸弹攻防

技巧1 初识网络炸弹

技巧2 网络炸弹都有哪些种类

技巧3 网络炸弹攻击实例

<<电脑黑客攻防技巧>>

技巧4 防御网络炸弹

技巧5 清除网络标题栏被添加的非法信息

7.3 网络浏览器安全设置

技巧1 设置Internet安全级别

技巧2 禁止用户添加或删除安全区域中的站点

技巧3 设置“Internet 属性”对话框中选项卡的访问权限

技巧4 设置“常规”选项卡中的按钮是否可用

技巧5 设置“内容”选项卡中的按钮是否可用

技巧6 禁用“帮助”菜单

技巧7 启动浏览器时不加载任何页面

技巧8 设置隐私级别

技巧9 禁止更改安全区域设置

技巧10 过滤弹出广告页面

技巧11 禁止IE组件的自动安装

技巧12 禁用IE中鼠标右键功能

技巧13 打开仿冒网站筛选功能

技巧14 禁止更改浏览器的主页

技巧15 锁定IE的下载功能

技巧16 更改ActiveX文件下载存放的位置

技巧17 关闭网络时自动清空临时文件夹

技巧18 免疫3721等插件

技巧19 取消安全网页的缓存

技巧20 清除日常上网痕迹

技巧21 屏蔽网络自动完成功能

技巧22 允许IE对Windows Installer脚本的安全提示

第8章 QQ、MSN和E-mail 攻防

8.1 走近QQ攻击

技巧1 QQ的攻击方式

技巧2 做好QQ的防范策略

技巧3 QQ攻击的危害

8.2 QQ攻防实战

技巧1 使用阿拉QQ大盗

技巧2 QQ尾巴生成器

技巧3 QQ强制聊天

技巧4 QQ炸弹攻防剖析

技巧5 设置代理隐藏本地IP地址

技巧6 使用QQ医生扫描盗号木马

技巧7 加密QQ聊天记录

技巧8 将QQ彻底隐藏

<<电脑黑客攻防技巧>>

技巧9 文件接收安全设置

技巧10 自定义QQ接收文件的保存路径

技巧11 通过密码保护找回被盗的

QQ号码

技巧12 通过申诉找回QQ密码

技巧13 如何避免键盘记录器记录QQ

账号密码

技巧14 被盗QQ号中的好友恢复

技巧15 从源头杜绝黑客盗取QQ密码

8.3 MSN安全

技巧1 撤销MSN自动登录

技巧2 让杀毒软件自动扫描接收文件

技巧3 认识和清除“MSN密码窃贼”

技巧4 用另类方法保护MSN聊天记录

技巧5 在Windows Live Messenger中

隐藏IP地址

技巧6 自动拒绝不安全文件传输

技巧7 使用Windows OneCare安全扫描

程序

技巧8 加密Windows Live Messenger

联系人列表

技巧9 让MSN隐藏摄像头

技巧10 阻止不受欢迎的客人

技巧11 认识和清除“MSN性感鸡”

(MSN.DropBot.b)

技巧12 认识和清除“MSN小尾巴”

8.3 电子邮箱攻防

技巧1 常见的电子邮箱攻击手段

技巧2 电子邮件安全策略

技巧3 使用流光扫描器盗取邮箱

技巧4 禁止IE记录登录信息

技巧5 过滤垃圾邮件

技巧6 设置邮箱密码保护

技巧7 找回邮箱密码

技巧8 自动拒绝邮件炸弹

第9章 木马攻防

9.1 认识木马

技巧1 木马的特性与分类

技巧2 常见的木马类型

技巧3 木马的启动方式

技巧4 常用的木马入侵手段

技巧5 木马的伪装手段

技巧6 木马的防范策略

技巧7 电脑中木马病毒的主要途径

技巧8 电脑受到木马入侵后的表现

9.2 木马的制作

技巧1 制作chm电子书木马

<<电脑黑客攻防技巧>>

技巧2 制作软件捆绑木马

技巧3 制作自解压木马

9.3 预防木马入侵

技巧1 增强木马防范意识

技巧2 设置注册表权限防木马启动

技巧3 禁止硬盘AutoRun功能预防

木马运行

技巧4 禁用屏保预防木马运行

技巧5 防范反弹端口型木马

技巧6 分离带木马的文件

9.4 使用软件查杀木马程序

技巧1 使用金山网盾防御木马程序

技巧2 使用金山卫士查杀木马程序

技巧3 使用木马克星查杀木马程序

技巧4 使用Windows木马清道夫

清除木马

技巧5 使用360安全卫士查杀木马

程序

9.5 手工清除木马实例

技巧1 清除冰河木马

技巧2 清除机器狗系列木马

技巧3 清除网游盗号木马

技巧4 清除“广外女生”木马

技巧5 清除“QQSPY密码间谍”

木马

技巧6 清除“WAY”木马

第10章 防范电脑病毒

10.1 了解计算机病毒

技巧1 初识电脑病毒

技巧2 电脑病毒的预防

技巧3 如何判断是否中了病毒

10.2 手动查毒与防毒

技巧1 利用BIOS设置防毒

技巧2 根据进程查杀病毒

技巧3 设置注册表权限防病毒启动

技巧4 使用在线病毒检测

技巧5 清除新型病毒

技巧6 巧用故障恢复控制台删除病毒

技巧7 图片病毒的防范

技巧8 利用批处理文件防范病毒

技巧9 防范移动存储设备传播病毒

10.3 常见杀毒软件应用

技巧1 使用瑞星杀毒软件

技巧2 使用江民杀毒软件

技巧3 使用卡巴斯基杀毒软件

技巧4 使用金山毒霸杀毒软件

技巧5 使用杀毒软件要提高警惕

<<电脑黑客攻防技巧>>

技巧6 查杀电脑病毒的注意事项

10.4 清除常见病毒实例

技巧1 感染“熊猫烧香”病毒后的处理方法

技巧2 感染“威金”病毒后的处理方法

技巧3 清除“QQ消息连发器”病毒

技巧4 清除“神速”木马

技巧5 清除“Zotob”狙击波病毒

技巧6 清除“爱情森林”病毒

技巧7 “爱情森林”病毒变种一的清除

技巧8 “爱情森林”病毒变种二的清除

技巧9 “爱情森林”病毒变种三的清除

技巧10 “爱情森林”病毒变种四的清除

10.5 U盘病毒的预防与查杀

技巧1 查杀U盘病毒

技巧2 使用金山毒霸查杀U盘病毒

技巧3 手动查杀U盘病毒

第11章 防范流氓软件与间谍软件

11.1 认识流氓软件与间谍软件

技巧1 与流氓软件零距离接触

技巧2 初步认识间谍软件

11.2 防范与清除流氓软件

技巧1 防范流氓软件

技巧2 使用超级兔子清理流氓软件

技巧3 使用瑞星卡卡清理流氓软件

技巧4 使用金山卫士清理流氓软件

技巧5 Windows流氓软件清理大师的使用

11.3 防范与清除间谍软件

技巧1 使用Spy Sweeper清除间谍软件

技巧2 使用事件查看器查找本机间谍软件

技巧3 使用Windows Defender查杀间谍软件

技巧4 清除流氓软件和间谍软件应该注意的问题

技巧5 防止间谍软件的其他措施

11.4 遭遇恶意代码和流氓软件后的修复

技巧1 默认主页被修改

技巧2 默认首页被修改

技巧3 主页设置被屏蔽锁定，且设置选项不可更改

技巧4 默认的IE搜索引擎被修改

技巧5 IE标题栏被添加非法信息

技巧6 鼠标右键菜单被添加非法网站链接

<<电脑黑客攻防技巧>>

技巧7 禁用鼠标右键弹出菜单功能

技巧8 锁定地址栏的下拉菜单并添加文字信息提示

技巧9 IE “查看”菜单下的“源文件”项被禁用

<<电脑黑客攻防技巧>>

章节摘录

版权页：插图：网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网上传输的信息，也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获网上的数据，这是黑客使用最多的方法，但是，网络监听只能应用于物理上连接于同一网段的主机，通常被用于获取用户口令。

2.后门程序在程序员设计一些功能复杂的程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块分别进行设计、调试，这时的后门就是一个模块的秘密入口。

在程序开发阶段，后门便于测试、更改和增强模块功能。

正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去掉，一些别有用心的人会利用“穷举搜索法”发现并利用这些后门，然后进入系统并发动攻击。

3.IP地址欺骗IP地址欺骗攻击是黑客们假冒受信主机目标进行的攻击。

在这种攻击中，受信主机是指拥有管理控制权限的主机或明确做出“信任”决定允许其访问自己网络的主机。

通常，这种IP地址欺骗攻击局限于把数据或命令注入到客户机/服务器应用之间，或对等网络连接传送中已存在的数据流。

为了达到双向通信，攻击者必须改变指向被欺骗IP地址的所有路由表。

4.信息炸弹信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。

比如向没有安装补丁的Windows系统发送特定组合的UDP数据包，会导致目标系统死机或重启；向某型号的路由器发送特定数据包致使路由器死机；向某人的电子邮件发送大量的垃圾邮件将此邮箱“撑爆”等。

目前常见的信息炸弹有邮件炸弹、逻辑炸弹等。

5.拒绝服务“拒绝服务”又叫分布式DOS攻击，它是使用超出被攻击目标处理能力的大量数据包消耗系统的可用系统、带宽资源，最后导致网络服务瘫痪的一种攻击手段。

<<电脑黑客攻防技巧>>

编辑推荐

《技高一筹:电脑黑客攻防技巧(双色)》：你来问，我来答。

《电脑直通车》在手，学习电脑不再困难！

以提问的方式进行讲解，均是电脑用户经常遇到的现实问题，系统地将需要学习的知识点串在一起，既相互关联，又相互独立。

配套光盘使用说明：将光盘印有文字的一面朝上放入电脑的CD或DVD光驱，稍后光盘会自动运行，并进入光盘主界面。

如果光盘没有自动运行，打开WindowsXP操作系统的“我的电脑”窗口（Windows7操作系统的“计算机”窗口），浏览光盘内容，双击Autorun.exe启动光盘并进入主界面。

在主界面的课程目录中选择需要学习的内容，并在弹出的窗口中单击课程名称，即可开始学习相应课程。

1课程目录，选择并进入相应课程、2查看丛书各新书简介、3查看光盘赠品与配套资源、4退出光盘。

1当前讲解内容文字、2播放控制按钮、3进入边学边练模式、4返回主界面。

图书配套光盘不但包含数小时精彩多媒体视频教程，还赠送200多部电脑知识视频教程（需网络下载）、多本电脑应用速查电子手册、“金山打字通”打字练习软件、万能五笔输入法……收录大量必备操作知识和实用技巧，覆盖电脑用户最常接触的领域。

电脑操作知识的精华提炼，条目化整理，助您在短时间内掌握实用技能。

各知识点既可独立学习，随查随用，即学即会；又可多知识点连贯起来进行系统化学习，全面掌握各方面应用。

<<电脑黑客攻防技巧>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>