

# 《电脑安全与黑客攻防从新手到高手》

## 图书基本信息

书名：《电脑安全与黑客攻防从新手到高手》

13位ISBN编号：9787030340788

10位ISBN编号：7030340787

出版时间：2012-6

出版社：科学出版社

作者：前沿文化

页数：308

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu111.com](http://www.tushu111.com)

# 《电脑安全与黑客攻防从新手到高手》

## 内容概要

《电脑安全与黑客攻防从新手到高手(全彩)》针对初学者的需求，全面、详细地讲解了电脑安全保障与黑客攻防的基本方法、疑难问题与相关技巧。图书在讲解上图文并茂，重视操作技巧的传授，并在图片中清晰地标注出要进行操作的位置与操作内容，并对重点、难点操作均配有视频教程，以求您能高效、完整地掌握本书内容。

《电脑安全与黑客攻防从新手到高手(全彩)》共分为16章，包括网络安全初接触、了解随处可见的计算机病毒、揭开黑客与木马的面纱、掌握Windows系统的漏洞和防范妙招、黑客常用命令详解、搜集远程计算机的信息、远程入侵计算机、木马入侵与防御、QQ攻击与防御、电子邮箱攻击与防御、来自网页的攻击与防御方法、防范扫描与恶意软件、网站攻防入门、网站上传漏洞的攻击和防御、网站脚本注入的攻击与防御等内容。

《电脑安全与黑客攻防从新手到高手(全彩)》既可供想要学习电脑安全保障与黑客攻防的用户使用，同时也可以作为电脑培训班的培训教材或学习辅导书。

## 书籍目录

### "目录

- Chapter 01 网络安全初接触 001
  - 1.1 网络安全 002
    - 1.1.1 网络安全的目的及保护范围 002
    - 1.1.2 现有的网络攻击/防御手段 003
    - 1.1.3 网络安全的四大方面 004
    - 1.1.4 通过管理保护网络安全 005
    - 1.1.5 网络安全的实施目的 008
  - 1.2 了解常见的不安全因素 010
    - 1.2.1 由网络系统本身带来的不安全因素 010
    - 1.2.2 网络外部的不安全因素 012
    - 1.2.3 网络不安全的原因 014
  - 1.3 认识网络安全的现状和发展趋势 016
    - 1.3.1 网络安全的现状 016
    - 1.3.2 网络安全的发展趋势 017
- Chapter 02 了解随处可见的计算机病毒 019
  - 2.1 计算机病毒的前世今生 020
    - 2.1.1 什么是计算机病毒 020
    - 2.1.2 计算机病毒起源何方 020
    - 2.1.3 计算机病毒的发展历程 021
    - 2.1.4 计算机病毒有哪些类型 025
    - 2.1.5 计算机病毒的命名规则 028
    - 2.1.6 解析计算机病毒的结构 028
    - 2.1.7 计算机病毒的特征 031
  - 2.2 计算机病毒如何作恶 032
    - 2.2.1 计算机中毒后的表现 032
    - 2.2.2 如何防范计算机病毒 034
  - 2.3 常见计算机病毒类型详解 036
    - 2.3.1 引导型病毒 036
    - 2.3.2 文件型病毒 037
    - 2.3.3 宏病毒 038
    - 2.3.4 蠕虫病毒 039
- Chapter 03 揭开黑客与木马的面纱 041
  - 3.1 什么是黑客 042
    - 3.1.1 “尼奥”们的由来 042
    - 3.1.2 黑客和骇客的区别 043
    - 3.1.3 黑客活动历史 044
    - 3.1.4 我国黑客发展历程 046
  - 3.2 黑客攻击的类型与动机 047
    - 3.2.1 攻击目的 047
    - 3.2.2 攻击动机 049
  - 3.3 木马的历史渊源 050
    - 3.3.1 希腊美女海伦与木马 050
    - 3.3.2 什么是计算机木马 050
    - 3.3.3 木马工作类型 054
    - 3.3.4 木马的发展历程 056
    - 3.3.5 经典木马介绍 057

- 3.4 木马的追踪与防范 059
  - 3.4.1 木马的追踪与反追踪技术 059
  - 3.4.2 木马的防范方法 060
- Chapter 04 掌握Windows系统的漏洞 062
  - 4.1 Windows系统的安全隐患 063
    - 4.1.1 Windows系统漏洞产生的原因 063
    - 4.1.2 Windows系统中的安全隐患 064
  - 4.2 Windows系统中的漏洞 067
    - 4.2.1 UPnP服务漏洞 067
    - 4.2.2 升级程序漏洞 068
    - 4.2.3 帮助和支持中心漏洞 068
    - 4.2.4 Windows Media Player漏洞 068
    - 4.2.5 压缩文件夹漏洞 069
    - 4.2.6 服务拒绝漏洞 069
    - 4.2.7 RDP漏洞 069
    - 4.2.8 VM漏洞 070
    - 4.2.9 热键漏洞 070
    - 4.2.10 账号快速切换漏洞 070
    - 4.2.11 输入法漏洞 071
    - 4.2.12 Unicode漏洞 071
    - 4.2.13 ISAPI缓冲区扩展溢出漏洞 072
    - 4.2.14 MS SQL Server的SA空密码漏洞 072
    - 4.2.15 系统管理权限漏洞 073
    - 4.2.16 路径优先漏洞 073
    - 4.2.17 NetDDE消息权限提升漏洞 074
    - 4.2.18 RDP拒绝服务漏洞 074
    - 4.2.19 域控制器拒绝服务漏洞 075
    - 4.2.20 事件查看器存在缓冲区溢出漏洞 075
    - 4.2.21 UDP套接字拒绝服务漏洞 075
    - 4.2.22 安全账户管理漏洞 075
    - 4.2.23 IIS 5.0的HTR映射远程堆溢出漏洞 076
    - 4.2.24 IIS 5.0的ASP缓冲溢出漏洞 076
    - 4.2.25 Narrator本地密码信息泄露漏洞 077
    - 4.2.26 SMTP认证漏洞 077
    - 4.2.27 IIS 5.0/5.1验证漏洞 077
    - 4.2.28 SQL Server函数库漏洞 077
    - 4.2.29 IIS 5.0伪造拒绝服务漏洞 078
    - 4.2.30 调试寄存器漏洞 078
    - 4.2.31 drwtsn32.exe文件漏洞 078
    - 4.2.32 快捷方式漏洞 079
    - 4.2.33 UTF漏洞 079
    - 4.2.34 IIS 5.0的SEARCH方法存在远程攻击漏洞 079
    - 4.2.35 Telnet漏洞 080
    - 4.2.36 LDAP漏洞 080
    - 4.2.37 IIS 5.0拒绝服务漏洞 081
    - 4.2.38 默认注册许可漏洞 081
    - 4.2.39 登录服务恢复模式存在空密码漏洞 081
    - 4.2.40 域账号锁定漏洞 082
    - 4.2.41 终端服务器登录缓存溢出漏洞 082

- 4.2.42 ActiveX参数漏洞 082
- 4.2.43 IIS 5.0 Cross Site Scripting漏洞 083
- 4.2.44 组策略漏洞 083
- 4.2.45 数字签名缓冲区溢出漏洞 083
- 4.3 针对漏洞的入侵方式 084
  - 4.3.1 数据驱动攻击 084
  - 4.3.2 伪造信息攻击 084
  - 4.3.3 针对信息协议弱点攻击 084
  - 4.3.4 登录欺骗 084
  - 4.3.5 利用系统管理员失误攻击 084
  - 4.3.6 重新发送攻击 085
  - 4.3.7 ICMP报文攻击 085
  - 4.3.8 针对源路径选项的弱点攻击 085
  - 4.3.9 以太网广播攻击 085
- 4.4 掌握常用的防护方法 085
  - 4.4.1 杀毒软件不可少 086
  - 4.4.2 个人防火墙不可替代 086
  - 4.4.3 分类设置复杂密码 086
  - 4.4.4 防止网络病毒与木马 086
  - 4.4.5 警惕“网络钓鱼” 087
  - 4.4.6 防范间谍软件 087
  - 4.4.7 只在必要时共享文件夹 087
  - 4.4.8 定期备份重要数据 087
- Chapter 05 Windows系统漏洞的防范妙招 088
  - 5.1 注册表安全防范技巧 089
    - 5.1.1 禁止访问和编辑注册表 089
    - 5.1.2 设置注册表防止系统隐私信息被泄露 090
    - 5.1.3 关闭默认共享保护系统安全 091
    - 5.1.4 设置登录警告 092
    - 5.1.5 隐藏桌面所有图标 092
    - 5.1.6 清理自动启动的程序 093
    - 5.1.7 禁用“刻录”功能 094
    - 5.1.8 删除“开始”菜单中的“文档”项 094
    - 5.1.9 删除查找结果中的文件列表 094
    - 5.1.10 在“我的电脑”中屏蔽磁盘驱动器图标 094
    - 5.1.11 清理访问“网上邻居”后留下的信息 095
    - 5.1.12 删除“运行”窗口中多余的选项 095
    - 5.1.13 在桌面上隐藏“网上邻居”图标 095
    - 5.1.14 禁止运行任何程序 096
    - 5.1.15 禁止远程修改注册表 096
  - 5.2 组策略安全登录设置 097
    - 5.2.1 设置休眠/挂起密码 097
    - 5.2.2 账户锁定策略 098
    - 5.2.3 密码策略 100
    - 5.2.4 禁止更改桌面设置 103
    - 5.2.5 隐藏“我的电脑”中指定的驱动器 103
    - 5.2.6 防止从“我的电脑”访问驱动器 103
    - 5.2.7 禁止使用命令提示符 104
    - 5.2.8 禁止更改显示属性 104

- 5.2.9 禁用注册表编辑器 104
- 5.2.10 彻底禁止访问“控制面板” 105
- 5.2.11 禁止建立新的拨号连接 105
- 5.2.12 禁用“添加/删除程序” 105
- 5.2.13 限制使用应用程序 105
- 5.3 设置系统中的各类密码 107
  - 5.3.1 设置Windows登录密码 107
  - 5.3.2 设置电源管理密码 108
  - 5.3.3 设置屏幕保护程序密码 109
- 5.4 掌握Windows XP的安全设置方法 111
  - 5.4.1 充分利用防火墙功能 111
  - 5.4.2 启用自动更新 112
  - 5.4.3 禁止病毒启动系统服务 112
  - 5.4.4 快速锁定计算机 113
- Chapter 06 黑客常用命令详解 115
  - 6.1 认识IP地址 116
    - 6.1.1 什么是IP地址 116
    - 6.1.2 IP地址的划分 116
    - 6.1.3 分配IP地址的机构 118
    - 6.1.4 公有IP地址与私有IP地址 118
  - 6.2 计算机通向外界的道路——端口 119
    - 6.2.1 端口的分类 119
    - 6.2.2 查看端口 121
    - 6.2.3 端口的关闭与限制 121
  - 6.3 黑客常用命令一览 124
    - 6.3.1 net命令 125
    - 6.3.2 远程登录命令telnet 127
    - 6.3.3 文件传输命令ftp 128
    - 6.3.4 添加计划任务命令at 129
    - 6.3.5 查看修改文件夹权限命令cacls 130
    - 6.3.6 回显命令echo 131
    - 6.3.7 命令行下的注册表操作 131
    - 6.3.8 查看当前系统用户情况命令query 132
    - 6.3.9 终止会话命令logoff 132
    - 6.3.10 物理网络查看命令ping 133
    - 6.3.11 网络配置查看命令ipconfig 134
    - 6.3.12 DNS查看命令nslookup 135
    - 6.3.13 地址解析命令arp 135
- Chapter 07 搜集远程计算机的信息 137
  - 7.1 搜集网络中的信息 138
    - 7.1.1 获取目标计算机的IP地址 138
    - 7.1.2 由IP地址获取目标计算机的地理位置 139
    - 7.1.3 了解网站备案信息 139
  - 7.2 检测系统漏洞 141
    - 7.2.1 什么是扫描器 141
    - 7.2.2 搜索共享资源 142
  - 7.3 端口扫描 143
    - 7.3.1 端口扫描的原理与分类 143
    - 7.3.2 端口扫描工具X-Scan 146

## Chapter 08 远程入侵计算机 148

### 8.1 基于认证的入侵 149

#### 8.1.1 IPC\$入侵 149

#### 8.1.2 Telnet入侵 155

#### 8.1.3 防范IPC\$连接入侵 161

### 8.2 利用注册表入侵 165

#### 8.2.1 开启远程注册表服务 165

#### 8.2.2 连接远程注册表 167

#### 8.2.3 通过注册表开启终端服务 168

### 8.3 常见问题解答 168

## Chapter 09 木马入侵与防御 170

### 9.1 深入了解木马 171

#### 9.1.1 木马常用的入侵手法 171

#### 9.1.2 深入了解木马的伪装手段 172

#### 9.1.3 识别木马有招数 174

#### 9.1.4 防范木马的入侵 175

### 9.2 木马的捆绑与使用 176

#### 9.2.1 使用Exebinder捆绑木马 176

#### 9.2.2 经典木马“冰河”的使用方法 179

## Chapter 10 QQ攻击与防御 183

### 10.1 远程攻击QQ 184

#### 10.1.1 强制聊天 184

#### 10.1.2 使用“QQ狙击手IpSniper”进行IP探测 185

#### 10.1.3 使用QQ炸弹攻击器进行信息轰炸 186

### 10.2 本地入侵QQ 187

#### 10.2.1 使用QQ聊天记录器记录聊天内容 187

#### 10.2.2 强行查看本地QQ聊天记录 188

#### 10.2.3 破解本地QQ密码 189

### 10.3 QQ防御术 190

#### 10.3.1 防止QQ密码被破解 190

#### 10.3.2 防范IP地址被探测 192

#### 10.3.3 防范QQ炸弹和木马 193

## Chapter 11 电子邮箱攻击与防御 195

### 11.1 获取电子邮箱密码的常用方法 196

#### 11.1.1 使用“流光”软件探测邮箱账号与密码 196

#### 11.1.2 使用“溯雪”软件获取邮箱密码 200

#### 11.1.3 使用“Email网页神抓”软件大批量获取邮箱地址 203

#### 11.1.4 对付密码探测的方法 204

### 11.2 电子邮箱攻击手段与防范 207

#### 11.2.1 使用邮箱炸弹进行攻击 207

#### 11.2.2 对付邮箱攻击的方法 207

## Chapter 12 来自网页的攻击与防御方法 211

### 12.1 了解恶意代码 212

#### 12.1.1 恶意代码的特征 212

#### 12.1.2 非过滤性病毒 212

#### 12.1.3 恶意代码的传播方式 213

#### 12.1.4 恶意代码的传播趋势 214

### 12.2 解除恶意代码对注册表的攻击 215

- 12.2.1 开机后自动弹出网页 215
- 12.2.2 浏览网页注册表被禁用 215
- 12.2.3 IE标题栏、默认首页被强行修改 216
- 12.2.4 默认的微软主页被修改 216
- 12.2.5 主页设置被屏蔽锁定且设置选项无效不可更改 216
- 12.2.6 默认的IE搜索引擎被修改 217
- 12.2.7 IE标题栏被添加广告信息 217
- 12.2.8 Outlook标题栏被添加广告信息 218
- 12.2.9 IE右键菜单被添加非法网站链接 218
- 12.2.10 单击鼠标右键弹出菜单功能被禁用 218
- 12.2.11 地址栏的下拉菜单被锁定并被添加文字信息 219
- 12.2.12 IE“查看”菜单下的“源文件”项被禁用 219
- 12.2.13 系统启动时弹出对话框 219
- 12.3 危险的IE浏览器 219
  - 12.3.1 IE炸弹攻击类型与后果 220
  - 12.3.2 对IE炸弹的防范与补救 220
- 12.4 网页攻击与防范实例 222
  - 12.4.1 常见ASP脚本攻击与防范 222
  - 12.4.2 跨站攻击和防范 222
- Chapter 13 防范扫描与恶意软件 225
  - 13.1 保护IP和端口 226
    - 13.1.1 设置代理服务器 226
    - 13.1.2 关闭端口 227
    - 13.1.3 配置安全策略保护端口 228
  - 13.2 清除恶意广告软件 233
    - 13.2.1 使用Ad-Aware驱逐恶意广告软件 234
    - 13.2.2 使用安博士软件驱逐恶意广告 235
  - 13.3 清除木马 235
    - 13.3.1 使用Windows任务管理器管理进程 236
    - 13.3.2 使用Trojan Remover清除木马 238
    - 13.3.3 使用Unlocker删除顽固木马文件 239
    - 13.3.4 使用360安全卫士维护系统安全 240
- Chapter 14 网站攻防入门 242
  - 14.1 网站安全详解 243
    - 14.1.1 网络攻击与网站 243
    - 14.1.2 网站安全与“肉鸡” 243
    - 14.1.3 动态网站与网站安全 244
    - 14.1.4 数据库与网站安全 245
    - 14.1.5 SQL与网站安全 248
    - 14.1.6 Web 2.0网站与黑客 249
    - 14.1.7 网站服务 249
    - 14.1.8 客户端交互技术Ajax 250
  - 14.2 网站的结构和组成 251
    - 14.2.1 网站系统基本架构 251
    - 14.2.2 网站工作原理 252
    - 14.2.3 网站服务器 252
    - 14.2.4 网页浏览器 252

- 14.3 网页程序开发语言分类 252
  - 14.3.1 服务器端开发语言 252
  - 14.3.2 客户端开发语言 253
- 14.4 网站程序运行的常见环境 254
  - 14.4.1 Windows下的网站运行平台 255
  - 14.4.2 Linux下的网站运行平台 255
- 14.5 网站程序常见错误提示的含义 257
  - 14.5.1 HTTP错误提示含义 258
  - 14.5.2 FTP错误提示含义 260
- 14.6 网站程序数据通信方式 262
  - 14.6.1 URL与HTTP/HTTPS协议 262
  - 14.6.2 Cookies与Session 264
  - 14.6.3 GET与POST数据提交 264
  - 14.6.4 常用字符集分类 265
- 14.7 网站程序数据加密方式 266
  - 14.7.1 MD5加密 267
  - 14.7.2 SHA1加密 268
  - 14.7.3 Base64加密 268
  - 14.7.4 Zend加密 269
  - 14.7.5 ASP代码加密工具 269
- 14.8 常见网站漏洞一览 270
- Chapter 15 网站上传漏洞的攻击和防御 271
  - 15.1 上传漏洞存在的原因 272
  - 15.2 各种类型的上传漏洞 273
    - 15.2.1 上传路径过滤不严导致的漏洞 274
    - 15.2.2 上传文件类型变量过滤不严造成的漏洞 276
    - 15.2.3 文件名过滤不严造成的漏洞 278
    - 15.2.4 逻辑错误产生的漏洞 279
  - 15.3 各种在线编辑器漏洞 281
    - 15.3.1 突破图片预览的限制 282
    - 15.3.2 突破禁止创建.asp文件夹的限制 282
    - 15.3.3 增加上传图片类型 283
    - 15.3.4 反过滤上传 284
  - 15.4 上传漏洞的防御 284
    - 15.4.1 下载官方补丁 284
    - 15.4.2 找网站开发商修改程序来防御上传漏洞 286
    - 15.4.3 换用其他编辑器的方法来防御上传漏洞 286
    - 15.4.4 用手动法来防御上传漏洞 286
- Chapter 16 网站脚本注入的攻击与防御 288
  - 16.1 深入剖析脚本注入攻击 289
    - 16.1.1 注入攻击核心原理 289
    - 16.1.2 形式各异的注入攻击分类 289
    - 16.1.3 SQL注入攻击特点 289
    - 16.1.4 注入攻击流程详解 290
  - 16.2 注入攻击的基础 292
    - 16.2.1 数据库知识 292
    - 16.2.2 SQL注入与数据库 294
  - 16.3 注入漏洞案例剖析 300
    - 16.3.1 ASP注入漏洞案例分析 300

16.3.2 ASPX注入漏洞案例分析 301

16.3.3 PHP注入漏洞案例分析 303

16.4 防御注入攻击 306

16.4.1 提高编程水平 306

16.4.2 提高密码的复杂程度 307

16.4.3 善用防注入工具 307

"

# 《电脑安全与黑客攻防从新手到高手》

## 精彩短评

- 1、书的质量很好，每一本都有光盘，内容详细。
- 2、有点难，不过我喜欢
- 3、地方的
- 4、东西不错，包装再严格点更好，加油吧
- 5、还不错。。知识比较基础。
- 6、????????????????????

# 《电脑安全与黑客攻防从新手到高手》

## 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:[www.tushu111.com](http://www.tushu111.com)