

<<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

出版时间：科学出版社

作者：前沿文化

页数：308

字数：443000

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>

## 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。

本书共分为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。

本书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

Chapter 01 网络安全初接触

1.1 网络安全

1.1.1 网络安全的目的及保护范围

1.1.2 现有的网络攻击/防御手段

1.1.3 网络安全的四大方面

1.1.4 通过管理保护网络安全

1.1.5 网络安全的实施目的

1.2 了解常见的不安全因素

1.2.1 由网络系统本身带来的不安全因素

1.2.2 网络外部的不安全因素

1.2.3 网络不安全的原因

1.3 认识网络安全的现状和发展趋势

1.3.1 网络安全的现状

1.3.2 网络安全的发展趋势

Chapter 02 了解随处可见的计算机病毒

2.1 计算机病毒的前世今生

2.1.1 什么是计算机病毒

2.1.2 计算机病毒起源何方

2.1.3 计算机病毒的发展历程

2.1.4 计算机病毒有哪些类型

2.1.5 计算机病毒的命名规则

2.1.6 解析计算机病毒的结构

2.1.7 计算机病毒的特征

2.2 计算机病毒如何作恶

2.2.1 计算机中毒后的表现

2.2.2 如何防范计算机病毒

2.3 常见计算机病毒类型详解

2.3.1 引导型病毒

2.3.2 文件型病毒

2.3.3 宏病毒

2.3.4 蠕虫病毒

Chapter 03 揭开黑客与木马的面纱

3.1 什么是黑客

3.1.1 “尼奥”们的由来

3.1.2 黑客和骇客的区别

3.1.3 黑客活动历史

3.1.4 我国黑客发展历程

3.2 黑客攻击的类型与动机

3.2.1 攻击目的

3.2.2 攻击动机

3.3 木马的历史渊源

3.3.1 希腊美女海伦与木马

3.3.2 什么是计算机木马

3.3.3 木马工作类型

3.3.4 木马的发展历程

3.3.5 经典木马介绍

3.4 木马的追踪与防范

3.4.1 木马的追踪与反追踪技术

3.4.2 木马的防范方法

Chapter 04 掌握Windows系统的漏洞

4.1 Windows系统的安全隐患

4.1.1 Windows系统漏洞产生的原因

4.1.2 Windows系统中的安全隐患

4.2 Windows系统中的漏洞

4.2.1 UPnP服务漏洞

4.2.2 升级程序漏洞

4.2.3 帮助和支持中心漏洞

4.2.4 Windows Media Player漏洞

4.2.5 压缩文件夹漏洞

4.2.6 服务拒绝漏洞

4.2.7 RDP漏洞

4.2.8 VM漏洞

4.2.9 热键漏洞

4.2.10 账号快速切换漏洞

4.2.11 输入法漏洞

4.2.12 Unicode漏洞

4.2.13 ISAPI缓冲区扩展溢出漏洞

4.2.14 MS SQL Server的SA空密码漏洞

4.2.15 系统管理权限漏洞

4.2.16 路径优先漏洞

4.2.17 NetDDE消息权限提升漏洞

4.2.18 RDP拒绝服务漏洞

4.2.19 域控制器拒绝服务漏洞

4.2.20 事件查看器存在缓冲区溢出漏洞

4.2.21 UDP套接字拒绝服务漏洞

4.2.22 安全账户管理漏洞

4.2.23 IIS 5.0的HTR映射远程堆溢出漏洞

4.2.24 IIS 5.0的ASP缓冲溢出漏洞

4.2.25 Narrator本地密码信息泄露漏洞

4.2.26 SMTP认证漏洞

4.2.27 IIS 5.0/5.1验证漏洞

4.2.28 SQL Server函数库漏洞

4.2.29 IIS 5.0伪造拒绝服务漏洞

4.2.30 调试寄存器漏洞

4.2.31 drwtsn32.exe文件漏洞

4.2.32 快捷方式漏洞

4.2.33 UTF漏洞

4.2.34 IIS 5.0的SEARCH方法存在远程攻击漏洞

4.2.35 Telnet漏洞

4.2.36 LDAP漏洞

4.2.37 IIS 5.0拒绝服务漏洞

4.2.38 默认注册许可漏洞

- 4.2.39 登录服务恢复模式存在空密码漏洞
- 4.2.40 域账号锁定漏洞
- 4.2.41 终端服务器登录缓存溢出漏洞
- 4.2.42 ActiveX参数漏洞
- 4.2.43 IIS 5.0 Cross Site Scripting漏洞
- 4.2.44 组策略漏洞
- 4.2.45 数字签名缓冲区溢出漏洞
- 4.3 针对漏洞的入侵方式
  - 4.3.1 数据驱动攻击
  - 4.3.2 伪造信息攻击
  - 4.3.3 针对信息协议弱点攻击
  - 4.3.4 登录欺骗
  - 4.3.5 利用系统管理员失误攻击
  - 4.3.6 重新发送攻击
  - 4.3.7 ICMP报文攻击
  - 4.3.8 针对源路径选项的弱点攻击
  - 4.3.9 以太网广播攻击
- 4.4 掌握常用的防护方法
  - 4.4.1 杀毒软件不可少
  - 4.4.2 个人防火墙不可替代
  - 4.4.3 分类设置复杂密码
  - 4.4.4 防止网络病毒与木马
  - 4.4.5 警惕“网络钓鱼”
  - 4.4.6 防范间谍软件
  - 4.4.7 只在必要时共享文件夹
  - 4.4.8 定期备份重要数据

#### Chapter 05 Windows系统漏洞的防范妙招

- 5.1 注册表安全防范技巧
  - 5.1.1 禁止访问和编辑注册表
  - 5.1.2 设置注册表防止系统隐私信息被泄露
  - 5.1.3 关闭默认共享保护系统安全
  - 5.1.4 设置登录警告
  - 5.1.5 隐藏桌面所有图标
  - 5.1.6 清理自动启动的程序
  - 5.1.7 禁用“刻录”功能
  - 5.1.8 删除“开始”菜单中的“文档”项
  - 5.1.9 删除查找结果中的文件列表
  - 5.1.10 在“我的电脑”中屏蔽磁盘驱动器图标
  - 5.1.11 清理访问“网上邻居”后留下的信息
  - 5.1.12 删除“运行”窗口中多余的选项
  - 5.1.13 在桌面上隐藏“网上邻居”图标
  - 5.1.14 禁止运行任何程序
  - 5.1.15 禁止远程修改注册表
- 5.2 组策略安全登录设置
  - 5.2.1 设置休眠/挂起密码
  - 5.2.2 账户锁定策略
  - 5.2.3 密码策略

- 5.2.4 禁止更改桌面设置
- 5.2.5 隐藏“我的电脑”中指定的驱动器
- 5.2.6 防止从“我的电脑”访问驱动器
- 5.2.7 禁止使用命令提示符
- 5.2.8 禁止更改显示属性
- 5.2.9 禁用注册表编辑器
- 5.2.10 彻底禁止访问“控制面板”
- 5.2.11 禁止建立新的拨号连接
- 5.2.12 禁用“添加/删除程序”
- 5.2.13 限制使用应用程序
- 5.3 设置系统中的各类密码
  - 5.3.1 设置Windows登录密码
  - 5.3.2 设置电源管理密码
  - 5.3.3 设置屏幕保护程序密码
- 5.4 掌握Windows XP的安全设置方法
  - 5.4.1 充分利用防火墙功能
  - 5.4.2 启用自动更新
  - 5.4.3 禁止病毒启动系统服务
  - 5.4.4 快速锁定计算机
- Chapter 06 黑客常用命令详解
  - 6.1 认识IP地址
    - 6.1.1 什么是IP地址
    - 6.1.2 IP地址的划分
    - 6.1.3 分配IP地址的机构
    - 6.1.4 公有IP地址与私有IP地址
  - 6.2 计算机通向外界的道路--端口
    - 6.2.1 端口的分类
    - 6.2.2 查看端口
    - 6.2.3 端口的关闭与限制
  - 6.3 黑客常用命令一览
    - 6.3.1 net命令
    - 6.3.2 远程登录命令telnet
    - 6.3.3 文件传输命令ftp
    - 6.3.4 添加计划任务命令at
    - 6.3.5 查看修改文件夹权限命令cacls
    - 6.3.6 回显命令echo
    - 6.3.7 命令行下的注册表操作
    - 6.3.8 查看当前系统用户情况命令query
    - 6.3.9 终止会话命令logoff
    - 6.3.10 物理网络查看命令ping
    - 6.3.11 网络配置查看命令ipconfig
    - 6.3.12 DNS查看命令nslookup
    - 6.3.13 地址解析命令arp
- Chapter 07 搜集远程计算机的信息
  - 7.1 搜集网络中的信息
    - 7.1.1 获取目标计算机的IP地址
    - 7.1.2 由IP地址获取目标计算机的地理位置

- 7.1.3 了解网站备案信息
- 7.2 检测系统漏洞
  - 7.2.1 什么是扫描器
  - 7.2.2 搜索共享资源
- 7.3 端口扫描
  - 7.3.1 端口扫描的原理与分类
  - 7.3.2 端口扫描工具X-Scan
- Chapter 08 远程入侵计算机
  - 8.1 基于认证的入侵
    - 8.1.1 IPC\$入侵
    - 8.1.2 Telnet入侵
    - 8.1.3 防范IPC\$连接入侵
  - 8.2 利用注册表入侵
    - 8.2.1 开启远程注册表服务
    - 8.2.2 连接远程注册表
    - 8.2.3 通过注册表开启终端服务
  - 8.3 常见问题解答
- Chapter 09 木马入侵与防御
  - 9.1 深入了解木马
    - 9.1.1 木马常用的入侵手法
    - 9.1.2 深入了解木马的伪装手段
    - 9.1.3 识别木马有招数
    - 9.1.4 防范木马的入侵
  - 9.2 木马的捆绑与使用
    - 9.2.1 使用Exebinder捆绑木马
    - 9.2.2 经典木马“冰河”的使用方法
- Chapter 10 QQ攻击与防御
  - 10.1 远程攻击QQ
    - 10.1.1 强制聊天
    - 10.1.2 使用“QQ狙击手IpSniper”进行IP探测
    - 10.1.3 使用QQ炸弹攻击器进行信息轰炸
  - 10.2 ?
  - 本地入侵QQ
    - 10.2.1 使用QQ聊天记录器记录聊天内容
    - 10.2.2 强行查看本地QQ聊天记录
    - 10.2.3 破解本地QQ密码
  - 10.3 QQ防御术
    - 10.3.1 防止QQ密码被破解
    - 10.3.2 防范IP地址被探测
    - 10.3.3 防范QQ炸弹和木马
- Chapter 11 电子邮箱攻击与防御
  - 11.1 获取电子邮箱密码的常用方法
    - 11.1.1 使用“流光”软件探测邮箱账号与密码
    - 11.1.2 使用“溯雪”软件获取邮箱密码
    - 11.1.3 使用“Email网页神抓”软件大批量获取邮箱地址
    - 11.1.4 对付密码探测的方法

## 11.2 电子邮箱攻击手段与防范

### 11.2.1 使用邮箱炸弹进行攻击

### 11.2.2 对付邮箱攻击的方法

## Chapter 12 来自网页的攻击与防御方法

### 12.1 了解恶意代码

#### 12.1.1 恶意代码的特征

#### 12.1.2 非过滤性病毒

#### 12.1.3 恶意代码的传播方式

#### 12.1.4 恶意代码的传播趋势

### 12.2 解除恶意代码对注册表的攻击

#### 12.2.1 开机后自动弹出网页

#### 12.2.2 浏览网页注册表被禁用

#### 12.2.3 IE标题栏、默认首页被强行修改

#### 12.2.4 默认的微软主页被修改

#### 12.2.5 主页设置被屏蔽锁定且设置选项无效不可更改

#### 12.2.6 默认的IE搜索引擎被修改

#### 12.2.7 IE标题栏被添加广告信息

#### 12.2.8 Outlook标题栏被添加广告信息

#### 12.2.9 IE右键菜单被添加非法网站链接

#### 12.2.10 单击鼠标右键弹出菜单功能被禁用

#### 12.2.11 地址栏的下拉菜单被锁定并被添加文字信息

#### 12.2.12 IE“查看”菜单下的“源文件”项被禁用

#### 12.2.13 系统启动时弹出对话框

### 12.3 危险的IE浏览器

#### 12.3.1 IE炸弹攻击类型与后果

#### 12.3.2 对IE炸弹的防范与补救

### 12.4 网页攻击与防范实例

#### 12.4.1 常见ASP脚本攻击与防范

#### 12.4.2 跨站攻击和防范

## Chapter 13 防范扫描与恶意软件

### 13.1 保护IP和端口

#### 13.1.1 设置代理服务器

#### 13.1.2 关闭端口

#### 13.1.3 配置安全策略保护端口

### 13.2 清除恶意广告软件

#### 13.2.1 使用Ad-Aware驱逐恶意广告软件

#### 13.2.2 使用安博士软件驱逐恶意广告

### 13.3 清除木马

#### 13.3.1 使用Windows任务管理器管理进程

#### 13.3.2 使用Trojan Remover清除木马

#### 13.3.3 使用Unlocker删除顽固木马文件

#### 13.3.4 使用360安全卫士维护系统安全

## Chapter 14 网站攻防入门

### 14.1 网站安全详解

#### 14.1.1 网络攻击与网站

#### 14.1.2 网站安全与“肉鸡”

#### 14.1.3 动态网站与网站安全



- 14.1.4 数据库与网站安全
- 14.1.5 SQL与网站安全
- 14.1.6 Web 2.0网站与黑客
- 14.1.7 网站服务
- 14.1.8 客户端交互技术Ajax
- 14.2 网站的结构和组成
  - 14.2.1 网站系统基本架构
  - 14.2.2 网站工作原理
  - 14.2.3 网站服务器
  - 14.2.4 网页浏览器
- 14.3 网页程序开发语言分类
  - 14.3.1 服务器端开发语言
  - 14.3.2 客户端开发语言
- 14.4 网站程序运行的常见环境
  - 14.4.1 Windows下的网站运行平台
  - 14.4.2 Linux下的网站运行平台
- 14.5 网站程序常见错误提示的含义
  - 14.5.1 HTTP错误提示含义
  - 14.5.2 FTP错误提示含义
- 14.6 网站程序数据通信方式
  - 14.6.1 URL与HTTP/HTTPS协议
  - 14.6.2 Cookies与Session
  - 14.6.3 GET与POST数据提交
  - 14.6.4 常用字符集分类
- 14.7 网站程序数据加密方式
  - 14.7.1 MD5加密
  - 14.7.2 SHA1加密
  - 14.7.3 Base64加密
  - 14.7.4 Zend加密
  - 14.7.5 ASP代码加密工具
- 14.8 常见网站漏洞一览
- Chapter 15 网站上传漏洞的攻击和防御
  - 15.1 上传漏洞存在的原因
  - 15.2 各种类型的上传漏洞
    - 15.2.1 上传路径过滤不严导致的漏洞
    - 15.2.2 上传文件类型变量过滤不严造成的漏洞
    - 15.2.3 文件名过滤不严造成的漏洞
    - 15.2.4 逻辑错误产生的漏洞
  - 15.3 各种在线编辑器漏洞
    - 15.3.1 突破图片预览的限制
    - 15.3.2 突破禁止创建.asp文件夹的限制
    - 15.3.3 增加上传图片类型
    - 15.3.4 反过滤上传
  - 15.4 上传漏洞的防御
    - 15.4.1 下载官方补丁
    - 15.4.2 找网站开发商修改程序来防御上传漏洞
    - 15.4.3 换用其他编辑器的方法来防御上传漏洞

15.4.4 用手动法来防御上传漏洞

Chapter 16 网站脚本注入的攻击与防御

16.1 深入剖析脚本注入攻击

16.1.1 注入攻击核心原理

16.1.2 形式各异的注入攻击分类

16.1.3 SQL注入攻击特点

16.1.4 注入攻击流程详解

16.2 注入攻击的基础

16.2.1 数据库知识

16.2.2 SQL注入与数据库

16.3 注入漏洞案例剖析

16.3.1 ASP注入漏洞案例分析

16.3.2 ASPX注入漏洞案例分析

16.3.3 PHP注入漏洞案例分析

16.4 防御注入攻击

16.4.1 提高编程水平

16.4.2 提高密码的复杂程度

16.4.3 善用防注入工具

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>