

## <<计算机使用安全与防护>>

### 图书基本信息

书名：<<计算机使用安全与防护>>

13位ISBN编号：9787121146633

10位ISBN编号：7121146630

出版时间：2011-9

出版时间：电子工业出版社

作者：徐津，胡晓菲，潘威 主编

页数：268

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>

## <<计算机使用安全与防护>>

### 内容概要

本书采用通俗易懂的方式介绍了计算机使用安全与防护所涉及的知识，精心选取典型的案例，系统地介绍如何降低网络威胁，提高计算机的使用安全系数。

本书以大量的实例对计算机使用安全防范设置进行详细的分析，并对一些需要注意的安全事项进行重点提示，在讲解过程中还加入一些安全防范技巧，旨在帮助读者了解计算机使用安全与防护领域的相关知识，建立计算机使用的安全意识，对保证计算机系统的安全具有实际的指导意义。

# <<计算机使用安全与防护>>

## 书籍目录

### 第1章 常用网络安全防御技术

#### 1.1 IE安全设置

- 1.1.1 清除上网痕迹
- 1.1.2 设置安全级别
- 1.1.3 阻止弹出窗口
- 1.1.4 禁用自动完成功能
- 1.1.5 禁止弹出式广告
- 1.1.6 直接进入精选网址
- 1.1.7 使用代理服务器上网
- 1.1.8 设置分级审查
- 1.1.9 改变IE临时文件大小
- 1.1.10 加速网页下载
- 1.1.11 禁止网站偷窃隐私
- 1.1.12 IE高级安全设置

#### 1.2 QQ安全设置

- 1.2.1 密码保护
- 1.2.2 加密聊天记录
- 1.2.3 设置身份验证
- 1.2.4 拒绝陌生人消息

#### 1.3 E-mail安全设置

- 1.3.1 邮箱密码的设置
- 1.3.2 使用多个邮箱
- 1.3.3 找回密码
- 1.3.4 邮箱安全防范
- 1.3.5 邮件病毒入侵后的清除步骤

#### 1.4 本章小结

#### 1.5 思考与练习

### 第2章 Windows常用安全设置

#### 2.1 组策略设置

- 2.1.1 组策略基础知识
- 2.1.2 组策略安全设置
- 2.1.3 开机策略
- 2.1.4 安全设置

#### 2.2 本地安全策略设置

- 2.2.1 打开方式
- 2.2.2 安全设置

#### 2.3 共享设置及常用网络测试命令

- 2.3.1 Windows XP系统中的共享设置
- 2.3.2 常用网络测试命令

#### 2.4 本章小结

#### 2.5 思考与练习

### 第3章 Windows系统漏洞检测工具

#### 3.1 漏洞的基本概念

#### 3.2 端口扫描

#### 3.3 网络和操作系统漏洞扫描器

## &lt;&lt;计算机使用安全与防护&gt;&gt;

- 3.3.1 认识扫描器
  - 3.3.2 漏洞扫描器概述
  - 3.3.3 漏洞扫描器的分类
  - 3.3.4 漏洞扫描器的用途
  - 3.3.5 漏洞扫描器的实现原理
  - 3.3.6 防御扫描的安全策略
  - 3.3.7 扫描器的使用策略
  - 3.4 扫描检测工具介绍
    - 3.4.1 X-Scan介绍
    - 3.4.2 金山毒霸漏洞扫描工具
    - 3.4.3 多线程扫描工具——X-way
    - 3.4.4 俄罗斯专业安全扫描软件——SSS
    - 3.4.5 SQL注入漏洞扫描器
    - 3.4.6 多线程IP、SNMP扫描器——Retina扫描器
    - 3.4.7 批量检测工具——MAC扫描器
    - 3.4.8 挖掘鸡
    - 3.4.9 瑞星漏洞扫描工具
    - 3.4.10 360安全卫士
    - 3.4.11 其他扫描器
  - 3.5 间谍软件检测工具
    - 3.5.1 拒绝潜藏的间谍软件
    - 3.5.2 Spybot的使用
  - 3.6 本章小结
  - 3.7 思考与练习
- 第4章 Windows系统安全加固技术
- 4.1 个人防火墙设置
    - 4.1.1 启用与禁用Windows防火墙
    - 4.1.2 设置Windows防火墙“例外”
    - 4.1.3 Windows防火墙的高级设置
    - 4.1.4 通过组策略设置Windows防火墙
    - 4.1.5 Windows防火墙的工作流程及注意事项
  - 4.2 账号和口令的安全设置
    - 4.2.1 账号的安全加固
    - 4.2.2 给账户双重加密
    - 4.2.3 创建密码重设盘
  - 4.3 文件系统安全设置
    - 4.3.1 文件和文件夹的加密
    - 4.3.2 在Windows下隐藏驱动器
  - 4.4 本章小结
  - 4.5 思考与练习
- 第5章 计算机病毒的检测和防范
- 5.1 计算机病毒概述
    - 5.1.1 计算机病毒的定义
    - 5.1.2 计算机病毒的发展历史
    - 5.1.3 计算机病毒的特点
    - 5.1.4 计算机病毒的危害及征兆
  - 5.2 计算机病毒的特征与分类

## <<计算机使用安全与防护>>

- 5.2.1 计算机病毒的特征
- 5.2.2 计算机病毒的分类
- 5.3 计算机病毒的机制
  - 5.3.1 计算机病毒的引导机制
  - 5.3.2 计算机病毒的发生机制
  - 5.3.3 计算机病毒的破坏机制
- 5.4 计算机病毒的检测与防范
  - 5.4.1 计算机病毒的检测
  - 5.4.2 计算机病毒的防范
- 5.5 特洛伊木马的检测与防范
  - 5.5.1 特洛伊木马的定义
  - 5.5.2 特洛伊木马的特征
  - 5.5.3 特洛伊木马的中毒状况
  - 5.5.4 特洛伊木马的检测
  - 5.5.5 特洛伊木马的防范
- 5.6 中毒后的系统恢复
- 5.7 本章小结
- 5.8 思考与练习
- 第6章 常用杀毒软件
  - 6.1 瑞星杀毒软件
    - 6.1.1 瑞星杀毒软件的安装
    - 6.1.2 瑞星杀毒软件的升级
    - 6.1.3 手动杀毒
    - 6.1.4 嵌入式杀毒
    - 6.1.5 监控功能
    - 6.1.6 主动防御功能
    - 6.1.7 瑞星账号保险柜
  - 6.2 金山毒霸
    - 6.2.1 病毒扫描
    - 6.2.2 综合设置
    - 6.2.3 U盘病毒免疫
  - 6.3 卡巴斯基杀毒软件
    - 6.3.1 设置卡巴斯基
    - 6.3.2 卡巴斯基使用技巧
  - 6.4 360杀毒软件
    - 6.4.1 病毒查杀
    - 6.4.2 360杀毒设置
    - 6.4.3 实时防护与升级
  - 6.5 本章小结
  - 6.6 思考与练习
- 第7章 常用黑客防御技术
  - 7.1 恶意网页代码技术
    - 7.1.1 网页恶意代码概述
    - 7.1.2 网页恶意代码的特点
    - 7.1.3 网页恶意代码攻击的形式
    - 7.1.4 恶意网页代码的修复与防范
  - 7.2 木马及其破解

## &lt;&lt;计算机使用安全与防护&gt;&gt;

- 7.2.1 木马的破解方式
  - 7.2.2 木马终结者
  - 7.3 防火墙技术
    - 7.3.1 Norton Personal Firewall
    - 7.3.2 BlackICE防火墙
    - 7.3.3 ZoneAlarm
    - 7.3.4 IE防火墙
    - 7.3.5 冰盾DDOS防火墙
    - 7.3.6 龙盾IIS防火墙
    - 7.3.7 天网防火墙
  - 7.4 其他安全工具
    - 7.4.1 奇虎360安全卫士
    - 7.4.2 IceSword冰刃
    - 7.4.3 AutoRuns
    - 7.4.4 Process Explorer
    - 7.4.5 Trojan Remover
    - 7.4.6 Loaris Trojan Remover
    - 7.4.7 Microsoft Baseline Security Analyzer (MBSA)
    - 7.4.8 KillBox
  - 7.5 本章小结
  - 7.6 思考与练习
- 第8章 轻松实现安全网络支付
- 8.1 淘宝密码安全设置
    - 8.1.1 设置密码保护
    - 8.1.2 修改账户密码
    - 8.1.3 找回丢失的密码
  - 8.2 支付宝密码安全设置
    - 8.2.1 修改支付宝密码
    - 8.2.2 开通手机动态口令
    - 8.2.3 找回丢失的支付宝密码
    - 8.2.4 其他支付宝安全设置
  - 8.3 网银账户安全设置
    - 8.3.1 使用电子口令卡
    - 8.3.2 使用U盾
  - 8.4 使用支付宝充值与付款
    - 8.4.1 为支付宝充值
    - 8.4.2 使用支付宝付款
  - 8.5 支付宝收款与提现
    - 8.5.1 使用支付宝收款
    - 8.5.2 从支付宝提现
  - 8.6 查看支付宝交易状况
    - 8.6.1 查询交易记录
    - 8.6.2 查询资金流动明细
    - 8.6.3 交易退款流程
  - 8.7 支付宝数字证书
    - 8.7.1 申请与安装数字证书
    - 8.7.2 备份数字证书

## <<计算机使用安全与防护>>

8.7.3 删除数字证书

8.7.4 导入数字证书

8.8 本章小结

8.9 思考与练习

### 第9章 计算机系统维护和数据恢复工具

9.1 备份和恢复

9.1.1 用Ghost备份和恢复系统

9.1.2 Windows系统的备份工具

9.1.3 Windows系统还原

9.1.4 蚂蚁驱动备份专家

9.1.5 Windows注册表的备份与恢复

9.1.6 专业级的Windows注册表优化和管理软件——Registry Help Pro

9.2 数据恢复工具

9.2.1 EasyRecovery

9.2.2 FinalData

9.2.3 R-Studio

9.2.4 CD DVD Data Recovery

9.2.5 RecoverMyFiles

9.3 本章小结

9.4 思考与练习

## &lt;&lt;计算机使用安全与防护&gt;&gt;

## 章节摘录

版权页：插图：按漏洞的成因分类，是对漏洞进行分类最令人头疼的一个话题。

因为对漏洞研究的不同抽象层次，会对同一个漏洞做出不同的分类。

对下面提到的ps竞争条件漏洞，从最低层次上来说参数验证错误，因为系统调用并没有检查它们所处理的是否为同一个对象。

从高一些的层次看，这是一个同步或竞争条件错误。

从更高的层次看，这则是一个逻辑错误，因为对象可能在使用过程中被删除。

至今也没看到一个比较完美的分类方案，包括一些专业的技术论坛网站上的分类也不能让人满意，现大致分成以下几类。

(1) 输入验证错误。

大多数的缓冲区溢出漏洞和cgi类漏洞都是由于未对用户提供的输入数据的合法性作适当的检查。

(2) 访问验证错误。

漏洞的产生是由于程序的访问验证部分存在某些可利用的逻辑错误，使绕过这种访问控制成为可能。

上面提到的那个早期AIX（UNIX操作系统）的rlogin（选程登录）漏洞就是这种典型。

(3) 竞争条件。

漏洞的产生在于程序处理文件等实体时在时序和同步方面存在问题，这处理的过程中可能存在一个机会窗口使攻击者能够施以外来的影响。

早期的Solaris系统的ps命令存在这种类型的漏洞，ps命令在执行的时候会在/tmp产生一个基于它系统进程的pid值的临时文件，然后把它chown（改变档案的拥有者）为root（超级用户），改名为ps\_data。

如果在ps命令运行时能够创建这个临时文件指向攻击者有兴趣的文件，这样ps命令执行以后，攻击者就可以对这个root拥有文件做任意的修改，这可以帮助攻击者获得root权限。

(4) 意外情况处置错误。

漏洞的产生在于程序在它的实现逻辑中没有考虑到一些意外情况，而这些意外情况是应该被考虑到的。

大多数的/tmp目录中的盲目跟随符号链接覆盖文件的漏洞属于这种类型。

临时文件一般都存储在/tmp目录中，该目录通常设置为任何人都可以读和写操作。

例如，Sco UNIX openserver的/etc/sysadm.d/bin/userOsa存在盲目覆盖调试日志文件的问题，而文件名是固定的，通过把文件名指向某些特权文件，可以完全破坏系统。

(5) 设计错误。

这个类别是非常笼统的，严格来说，大多数的漏洞存在都是设计错误，因此所有暂时无法放入到其他类别的漏洞。

(6) 配置错误。

漏洞的产生在于系统和应用的配置有误，或是软件安装在错误的地方，或是错误的配置参数，或是错误的访问权限，策略错误。

## <<计算机使用安全与防护>>

### 编辑推荐

《计算机使用安全与防护》是职业教育课程改革系列教材之一。

## <<计算机使用安全与防护>>

### 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>