

<<Windows系统漏洞攻击与安全>>

图书基本信息

书名：<<Windows系统漏洞攻击与安全防范实战>>

13位ISBN编号：9787900392770

10位ISBN编号：7900392777

出版时间：1970-1

出版时间：云南人民电子音像

作者：电脑报

页数：228

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>

## <<Windows系统漏洞攻击与安全>>

### 内容概要

《Windows系统漏洞攻击与安全防范实战（附光盘）》由电脑报总策划，并特邀资深IT图书撰稿人欧陪宗先生撰写。

欧先生长期担任多家数据恢复公司的技术顾问和某大型网站站长职务，是计算机安全实战技术行家。欧先生曾在《电脑报》、《中国计算机报》等多家国内知名IT媒体发表数据安全专文，已在十多家出版社出版过多部计算机专著，拥有丰富的书稿创作经验。

其代表作品有《Windows常见漏洞攻击与防范实战》、《电脑安全大师》、《黑客攻防36计》等。

## 书籍目录

第一篇 Windows常见漏洞详解第1章 Windows凭什么走列现在1.1 盖茨和他的微软1.2 起步岁月(1985 ~ 1994)1.2.1 Windows 1.01.2.2 Windows 2.x1.2.3 Windows 3.x1.2.4 Windows NT3.x1.3 迈向巅峰(1995 ~ 2000)1.3.1 Windows 951.3.2 Windows NT4.01.3.3 Windows 981.3.4 Windows 20001.3.5 Windows Me1.4 王者时代(2001 ~ 2007)1.4.1 Windows XP1.4.2 Windows Server 20031.4.3 Windows Vista1.4.5 Windows Server 20071.5 Windows未来发展的展望第2章 Windows系统存在的安全漏洞2.1 Windows漏洞攻击手段及防范2.1.1 Windows长扩展名存在缓冲溢出问题2.1.2 NetBIOS协议口令校验漏洞2.1.3 “畸形IPX NMPI报文”安全漏洞2.1.4 Cookies漏洞2.1.5 IE的安全隐患2.1.6 UPNP服务漏洞2.1.7 Windows本地登录验证漏洞2.1.8 SMB通讯协议漏洞2.1.9 拒绝服务攻击2.1.10 Windows拒绝服务攻击漏洞2.1.11 设备名称解析漏洞2.2 服务协议漏洞——Windows共享攻防实战.2.2.1 什么是SMB2.2.2 远程共享漏洞2.2.3 解除共享密码的几种方法2.2.4 系统设置共享后的必要安全防范2.2.5 用远程控制实现Windows文件共享2.3 OBB漏洞——Windows蓝屏攻击2.3.1 系统蓝屏工具2.3.2 蓝屏攻击的安全防范2.3.3 Windows系统蓝屏死机密码2.4 PWL漏洞——密码解除2.4.1 PWL文件的攻击与防范2.4.2 屏幕保护密码的攻击与防范2.4.3 解除PWL文件对Windows系统安全的危害第3章 Windows 2000漏洞攻防实战3.1 Windows 2000的安全性概述3.1.1 Windows 2000的安全性设计3.1.2 Windows 2000中的验证服务架构3.1.3 Windows 2000实现的安全特性3.1.4 Windows 2000“秘密武器”3.2 Windows 2000漏洞攻防措施3.2.1 Telnet漏洞3.2.2 本地操作漏洞3.2.3 登录漏洞3.2.4 NetBIOS的信息泄漏3.2.5 奇怪的系统崩溃特性3.2.6 IIS服务泄漏文件内容3.2.7 Unicode漏洞3.2.8 堵住Windows 2000 ICMP漏洞3.3 Windows 2000安全设置建议3.3.1 初级安全设置3.3.2 中级安全设置3.3.3 高级安全设置第4章 Windows XP漏洞攻防实战4.1 Windows XP的安全性概述4.2 Windows XP的漏洞攻防范措施4.2.1 UPNP漏洞4.2.2 账号锁定功能漏洞4.2.3 Windows XP远程桌面漏洞4.2.4 GDI拒绝服务漏洞4.2.5 终端服务IP地址欺骗漏洞4.2.6 防范措施4.3 Windows XP安全设置指南第5章 Windows NT漏洞攻防实战5.1 NT的安全策略5.1.1 用户账号和用户密码5.1.2 域名管理5.1.3 用户组权限5.1.4 共享资源权限5.2 NT在网络中的安全性5.3 NT攻击理论与防护实战5.3.1 NT内置组的权限5.3.2 NT默认状态下对目录的权限5.3.3 系统管理员管理工具的执行权限5.3.4 NT口令的脆弱性5.3.5 简单攻击NT的实例5.3.6 得到Windows NT管理权限后的攻击5.4 Windows NT漏洞攻防措施5.4.1 获取Administrator权限账号5.4.2 权限突破5.4.3 攻破SAM5.4.4 监听Windows NT密码验证交换过程5.5 入侵Windows NT常用工具5.5.1 Net命令5.5.2 Nat工具5.5.3 攻防实例第6章 Windows 2003漏洞攻防实战6.1 Windows 2003安全性概述6.2 Windows 2003漏洞解决方案6.2.1 取消正安全提示对话框6.2.2 重新支持ASP脚本6.2.3 清除默认共享隐患6.2.4 清空远程可访问的注册表路径6.2.5 关闭不必要的端口6.2.6 杜绝非法访问应用程序6.3 Windows 2003安全配置终极方案6.3.1 SERV.UFTP服务器的设置6.3.2 IIS的安全6.3.3 3389 终端服务器的安全配置6.3.4 FTP服务器配置6.3.5 把木马拒之门外6.4 Windows Server 2003防火墙设置6.4.1 基本设置6.4.2 测试基本设置6.4.3 高级设置第7章 Windows Vista漏洞攻防实战7.1 Windows Vista漏洞概述7.2 攻破Windows Vista登录口令的攻击7.2.1 详解Vista登录口令的秘密7.2.2 Google破解Vista登录口令7.2.3 防止快速破解Vista登录口令7.3 Windows Vista安全设置建议7.3.1 Vista自带防火墙设置7.3.2 安全软件设置第二篇 常被黑客利用的系统漏洞攻防实例第8章 常见木马漏洞攻击与防范实例8.1 木马的基本概念8.2 木马的定义8.2.1 远程控制型木马8.2.2 发送密码型木马8.2.3 破坏型木马8.2.4 FTP型木马8.3 揭开木马的神秘面纱8.3.1 木马的结构8.3.2 揭秘木马的攻击过程8.4 灰鸽子使用全攻略8.4.1 注册域名8.4.2 配置服务端程序8.4.3 制作网页木马8.4.4 JPG木马制作揭秘8.4.5 给灰鸽子木马加壳躲避查毒软件8.4.6 木马服务端的加壳保护8.4.7 灰鸽子的手工清除8.5 常见木马档案8.5.1 BO8.5.2 广外女生8.5.3 SBU 7黄金版8.5.4 黑洞8.5.5 聪明基因8.5.6 网络精灵8.5.7 无赖小子8.5.8 蓝色火焰8.6 木马隐形位置分析8.7 木马清除方法8.7.1 发现木马8.7.2 逮住黑客8.7.3 反黑在你的“爱机”种下木马的人8.7.4 清除木马8.8 木马的防范8.8.1 “中招”途径8.8.2 木马防范经验第9章 恶意代码漏洞攻击与防范9.1 解析恶意代码的特征与发展趋势9.1.1 恶意代码的特征9.1.2 非滤过性病毒9.1.3 恶意代码的传播手法9.1.4 恶意代码传播的趋势9.1.5 恶意代码相关的几个问题9.2 恶意代码人曝光9.2.1 浏览网页注册表被禁用9.2.2 篡改IE的默认页9.2.3 修改IE浏览器默认主页9.2.4 IE的默认首页灰色按钮不可选9.2.5 IE标题栏被修改9.2.6 IE右键菜单被修改9.2.7 IE默认搜索引擎被修改9.2.8 系统启动时弹出对话框9.2.9 IE默认连接首页被修改9.2.10 IE中鼠标右键失效9.2.11 查看

## &lt;&lt;Windows系统漏洞攻击与安全&gt;&gt;

“源文件”菜单被禁用9.2.12 浏览网页开始菜单被修改9.2.13 禁止鼠标右键9.2.14 共享你的硬盘9.3 打造完美的IE网页木马9.3.1 完美IE木马的特征9.3.2 IE木马的不足9.3.3 打造完美正木马9.4 恶意代码的预防

第10章 黑客常用漏洞攻击工具10.1 扫描之王——SSS10.1.1 SSS的功能介绍10.1.2 实例演示10.2 扫描利器——流光10.2.1 简单主机(漏洞)扫描10.2.2 高级漏洞扫描10.2.3 暴力破解10.3 专穿防火墙的反弹木马——DBB10.3.1 配置后门10.3.2 打开后门10.3.3 轻松操纵10.3.4 封杀后门10.4 反间谍软件——SS&D10.4.1 使用实战10.4.2 下载软件设防10.4.3 让系统具有“免疫”功能10.4.4 粉碎间谍程序10.4.5 查找启动项中的间谍10.5 系统监控器——Real Spy Monitor10.5.1 基本设置10.5.2 监控实战10.6 远程控制——PcAnywhere10.6.1 PcAnywhere安装10.6.2 PcAnywhere基本设置

第11章 基于网络的系统漏洞攻防实例11.1 宽带密码破解11.1.1 小心本地黑客11.1.2 远程盗取,防不胜防11.2 管理员帐户破解11.2.1 利用默认的Administrator11.2.2 创建密码恢复盘11.2.3 通过双系统删除SAM文件11.2.4 借助第三方密码恢复软件11.3 Snmp口令的利用11.3.1 什么是Snmp11.3.2 对Windows 2000进行刺探扫描11.3.3 Snmp浏览工具——IP Network Browser11.3.4 扫描工具——Languard Network Scanner11.3.5 防范基于Snmp的刺探扫描11.4 利用Google进行入侵与渗透11.4.1 攻击实战演练11.4.2 工具使用11.4.3 防范措施11.5 将入侵主机私有化11.5.1 私有型“肉鸡”的重要性11.5.2 “肉鸡”的要求11.5.3 “私有化”进程

第三篇 系统漏洞防范措施与技巧第12章 必知必会的网络漏洞安全基础知识12.1 扫清自己的足迹12.1.1 彻底地删除文件12.1.2 不留下蛛丝马迹12.1.3 隐藏文档内容12.1.4 清除临时文件12.1.5 保护重要文件12.1.6 改写网页访问历史记录12.1.7 清除输入的网址记录12.1.8 清除高速缓存中的信息12.2 保密知识初解12.2.1 密码保护12.2.2 防止在线入侵和病毒威胁12.2.3 使“用户配置文件”和“策略”12.2.4 两点小技巧12.3 认识系统进程12.3.1 明明白白系统进程12.3.2 关闭进程和重建进程12.3.3 查看进程的发起程序12.3.4 查看隐藏进程和远程进程12.3.5 杀死病毒进程12.4 巧妙识别真假Svchost.exe进程12.4.1 认识Svchost.exe进程12.4.2 识别Svchost.exe进程的真伪

第13章 堵住漏洞彻底剿除流氓软件与病毒13.1 认识“流氓软件”及其分类13.1.1 广告软件13.1.2 间谍软件13.1.3 浏览器劫持13.1.4 行为记录软件13.1.5 恶意共享软件13.2 诺顿网络安全特警13.2.1 配置安全特警13.2.2 启用诺顿网络安全特警13.2.3 程序扫描13.2.4 隐私控制13.2.5 在线安全检测13.2.6 封锁恶意IP13.2.7 端口安全防范13.3 360安全卫士查杀恶意软件13.3.1 系统漏洞修复13.3.2 查杀恶意软件13.3.3 全面系统诊断与修复13.3.4 免费查杀病毒13.4 微软反间谍高手13.4.1 初识反间谍软件利器13.4.2 手动扫描查杀间谍软件13.4.3 设置定时自动扫描13.4.4 开启实时监控13.5 瑞星卡卡根除“流氓软件”13.5.1 广告拦截13.5.2 系统修复13.5.3 病毒疫情实时监测13.6 金山系统清理专家13.6.1 恶意软件查杀13.6.2 两种方式修复IE13.6.3 进程和启动项管理13.6.4 历史痕迹清理13.6.5 其他特色功能介绍13.7 Windows流氓软件清理大师13.7.1 恶意软件卸载13.7.2 垃圾文件清理及系统优化13.7.3 四款特色安全工具

第14章 Windows的备份与恢复方案大全14.1 Windows 98的备份与恢复14.1.1 Windows 98的备份14.1.2 恢复Windows 9814.2 Windows 2000的备份与恢复14.2.1 备份Windows 200014.2.2 Windows 2000故障后的还原14.2.3 用系统紧急修复磁盘ERD14.2.4 用故障恢复控制台修复故障14.3 Windows XP的备份与恢复14.3.1 备份Windows XP14.3.2 Windows xP的紧急还原14.4 Windows Vista的备份与恢复14.4.1、Windows Vista自带备份恢复功能14.4.2 利用Ghost 10备份与恢复Vista14.4.3 利用安装文件备份与恢复Vista14.5 注册表的备份与恢复14.5.1 注册表的备份与恢复14.5.2 注册表急救术14.6 系统设置与文件的备份和恢复14.6.1 备份的内容14.6.2 备份的方法14.6.3 还原的方法14.6.4 驱动程序的备份

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>