

<<电脑硬道理 - 网络攻防>>

图书基本信息

书名：<<电脑硬道理 - 网络攻防>>

13位ISBN编号：9787894765925

10位ISBN编号：7894765929

出版时间：2011-6

出版时间：电脑报电子音像

作者：黄科

页数：320

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>

<<电脑硬道理 - 网络攻防>>

内容概要

网络攻击可以说是当今信息社会中不容忽视的独特现象，而目前大多数人的网络安全意识还很匮乏，在遇到别有用心者的入侵时不知道该如何应对。

本手册的主要目的就是让读者了解网络攻击的起源、常用工具以及攻击方式，并在熟悉基本网络安全知识的前提下，掌握基本的反黑知识、工具和修复技巧。

本手册是指导初学者快速掌握网络攻防的入门书籍，适用于广大网络爱好者，同时可作为一本速查手册，可用于网络安全从业人员及网络管理者。

<<电脑硬道理 - 网络攻防>>

书籍目录

网络攻击入门

- 1.1 初识网络攻击
- 1.2 认识IP地址
- 1.3 黑客的专用通道——端口
 - 1.3.1 什么是计算机端口
 - 1.3.2 端口的分类
 - 1.3.3 开启和关闭端口
 - 1.3.4 图形化的端口查看工具
- 1.4 木马的藏身之地——系统进程
 - 1.4.1 全面认识系统进程
 - 1.4.2 关闭进程和重建进程
 - 1.4.3 查看进程的发起程序
 - 1.4.4 查看隐藏进程和远程进程
 - 1.4.5 杀死病毒进程
- 1.5 系统服务与命令提示符
 - 1.5.1 系统服务
 - 1.5.2 命令提示符
- 1.6 字典和网络炸弹
 - 1.6.1 字典
 - 1.6.2 网络炸弹
- 1.7 日志文件攻防
 - 1.7.1 日志的特殊性
 - 1.7.2 为什么会对日志文件感兴趣
 - 扫描工具搜集重要信息
- 2.1 Sss扫描器扫描实战
 - 2.1.1 什么是扫描
 - 2.1.2 扫描实战
- 2.2 国产第一扫描器流光
 - 2.2.1 流光简介
 - 2.2.2 批量主机扫描
 - 2.2.3 指定漏洞扫描
- 2.3 自己查隐患X-scan应用实例
 - 2.3.1 X-scan的简介
 - 2.3.2 X-scan的基本使用
 - 2.3.3 高级设置
- 2.4 RPC漏洞扫描器
 - 2.4.1 RPC漏洞带来的危险
 - 2.4.2 深入浅出RPC
 - 2.4.3 扫描RPC漏洞
- 2.5 Webdavscan漏洞扫描器
 - 2.5.1 什么是WebDAV漏洞
 - 2.5.2 漏洞扫描实战
 - 2.5.3 解决方法
- 2.6 玩转NC监控与扫描功能
 - 2.6.1 监听本地计算机端口数据

<<电脑硬道理 - 网络攻防>>

- 2.6.2 监听远程计算机端口信息
- 2.6.3 将NC作为扫描器使用
- 2.7 扫描的反击与追踪
 - 2.7.1 使用Internet防火墙
 - 2.7.2 使用扫描监测工具
 - 2.7.3 让系统对Ping说“NO”
 - 嗅探器截取重要信息
- 3.1 嗅探器应用范围
- 3.2 Sniffer介绍
- 3.3 Iris网络嗅探器
 - 3.3.1 Iris的特点
 - 3.3.2 设置与使用Iris
 - 3.3.3 利用Iris捕获邮箱密码
 - 3.3.4 利用Iris捕获Telnet会话密码
- 3.4 网络间谍SpyNet Sniffer
- 3.5 艾菲网页侦探
- 3.6 看不见的网管专家
 - 3.6.1 Sniffer Portable功能简介
 - 3.6.2 查看捕获的报文
 - 3.6.3 捕获数据包后的分析工作
 - 3.6.4 设置捕获条件
- 3.7 嗅探应用实战
 - 反击QQ盗号者
- 3.8 防御Sniffer攻击
 - 3.7.1 怎样发现 Sniffer
 - 3.7.2 抵御Sniffer
- 3.9 使用屏幕间谍监视本地计算机
 - 系统漏洞攻防实例
- 4.1 认识系统漏洞攻防
 - 4.1.1 系统漏洞的基本概念
 - 4.1.2 系统漏洞的自动修补
- 4.2 漏洞攻防实例
 - 4.2.1 Messenger溢出工具
 - 4.2.2 Printer溢出工具IIS5Exploit
 - 4.2.3 Windows logon溢出工具体验
 - 4.2.4 动网论坛漏洞攻防揭秘
 - 4.2.5 DcomRpc漏洞溢出入侵与防范
- 4.3 系统漏洞检测与修复
 - 4.3.1 系统漏洞检测强大武器MBSA
 - 4.3.2 扫描局域网内计算机的安全漏洞
 - 4.3.3 消除共享漏洞的隐患
- 常用程序攻防
- 5.1 第三程序漏洞概述
 - 5.1.1 第三程序概述
 - 5.1.2 严峻的形势
- 5.2 Word Oday漏洞攻防
 - 5.2.1 漏洞简介

<<电脑硬道理 - 网络攻防>>

- 5.2.2 攻击实战
- 5.2.3 安全防范
- 5.3 动易漏洞利用实例
 - 5.3.1 问题所在
 - 5.3.2 入侵实战
- 5.4 Adobe Flash漏洞攻防
 - 5.4.1 入侵实例解析
 - 5.4.2 漏洞分析与防范
- 5.5 动网程序攻防实例
 - 5.5.1 入侵实例解析
 - 5.5.2 上传漏洞防范
- 5.6 EXCEL漏洞攻防
 - 5.6.1 漏洞简介
 - 5.6.2 入侵实例
 - 5.6.3 防范策略
- 5.7 Discuz论坛攻防
 - 5.7.1 准备工作
 - 5.7.2 入侵实例分析
- 5.8 Serv-U入侵攻防
 - 5.8.1 准备工作
 - 5.8.2 入侵实战
- 5.9 影视程序RealPlayer攻防
 - 5.9.1 入侵实例分析
 - 5.9.2 安全防范
- 5.10 博客程序L-BLOG攻防
 - 5.10.1 提权漏洞实战
 - 5.10.2 漏洞分析与防范
- 病毒与木马攻防实例
- 6.1 轻松判断电脑是否中毒
 - 6.1.1 安全工具不能运行
 - 6.1.2 在线杀毒网页不能打开
 - 6.1.3 常用文件打不开
 - 6.1.4 死机、提示内存不够
 - 6.1.5 键盘、鼠标、摄像头不听使唤
 - 6.1.6 任务管理器异常
 - 6.1.7 服务和自启动项异常
 - 6.1.8 硬盘灯、网卡灯狂闪
 - 6.1.9 QQ、MSN、网游等异常登录提醒
 - 6.1.10 查看CPU时间较大的程序
- 6.2 宏病毒及其防治方法
 - 6.2.1 认识宏
 - 6.2.2 宏病毒的判断方法
 - 6.2.3 宏病毒的防治和清除
- 6.3 邮件病毒识别与防治
 - 6.3.1 什么是邮件附件病毒
 - 6.3.2 邮件病毒的伪装方式
 - 6.3.3 多种方式防范邮件病毒

<<电脑硬道理 - 网络攻防>>

- 6.4 QQ群挂木马实例解析
 - 6.4.1 制作网页木马
 - 6.4.2 制作SWF木马
 - 6.4.3 在QQ群中挂马
- 6.5 QQ空间挂马剖析
 - 6.5.1 挂Flash木马
 - 6.5.2 挂网页木马
- 6.6 防范“文本文件”木马的破坏
 - 6.6.1 别被“文本”图标欺骗
 - 6.6.2 识别双后缀文件
 - 6.6.3 不会显示的文件名
 - 6.6.4 系统崩溃，毁于“碎片”
 - 6.6.5 精心构造的“文本陷阱”
 - 6.6.6 防范假“文本文件”
- 6.7 冰河陷阱欺骗术
 - 6.7.1 清除TxtFile型关联冰河
 - 6.7.2 卸载EXEFile关联冰河
- 6.8 DLL木马追踪与防范
 - 6.8.1 从DLL木马的DLL文件入手
 - 6.8.2 查看进程
 - 6.8.3 监控端口
 - 6.8.4 使用嗅探器来查看
 - 6.8.5 查看系统服务
- 6.9 能穿透防火墙的反弹木马
 - 6.9.1 配置后门
 - 6.9.2 打开后门
 - 6.9.3 轻松操纵
 - 6.9.4 封杀后门
- 6.10 木马“藏身”之地解析
 - 6.10.1 集成到程序中
 - 6.10.2 隐藏在配置文件中
 - 6.10.3 潜伏在Win.ini中
 - 6.10.4 伪装在普通文件中
 - 6.10.5 内置到注册表中
 - 6.10.6 隐蔽在Winstart.bat中
- 6.11 几招搞定“挂马”网站
 - 6.11.1 365门神搞定广告、恶意网站
 - 6.11.2 无忧电子眼屏蔽恶意网站
- 6.12 安全护盾保护电脑安全
 - 6.12.1 认识安全护盾
 - 6.12.2 设置安全护盾自动防御
 - 6.12.3 自动拦截与网络连接的程序
- 账户密码攻防实例
- 7.1 Administrator账户伪造
 - 7.1.1 更改账户名
 - 7.1.2 伪造陷阱账户
- 7.2 识破混迹管理员组的Guest账户

<<电脑硬道理 - 网络攻防>>

- 7.2.1 虚假的管理员账户
- 7.2.2 找出管理员组的Guest账户
- 7.2.3 Guest账户的安全管理
- 7.3 防范假终端管理员
 - 7.3.1 初步了解终端服务
 - 7.3.2 终端服务器的连接
 - 7.3.3 非法终端管理员的识别
- 7.4 系统密码攻防
 - 7.4.1 轻松破解Syskey双重加密
 - 7.4.2 BIOS密码设置与解除
 - 7.4.3 设置系统登录密码
 - 7.4.4 轻松找回管理员密码
 - 7.4.5 用ERD Commander恢复XP密码
- 7.5 办公文档密码攻防
 - 7.5.1 使用WordKey恢复Word密码
 - 7.5.3 轻松查看Excel文档密码
 - 7.5.4 WPS密码攻防
- 7.6 压缩文档密码攻防
 - 7.6.1 用RAR Password Cracker恢复RAR密码
 - 7.6.2 多功能密码破解软件
 - 7.6.3 暴力破解压缩文件密码
- 7.7 文件加密与解密
 - 7.7.1 与众不同的分时段加密
 - 7.7.2 图片加密好帮手
 - 7.7.3 文件分割巧加密
 - 7.7.4 生成自解密文件的“机器虫加密”
网络盗号与防范实例解析
- 8.1 QQ攻击与防范
 - 8.1.1 QQ安全配置
 - 8.1.2 “完美QQ大盗”攻防实例
 - 8.1.3 巧用工具软件防范QQ盗号
 - 8.1.4 QQ防盗应用技巧
 - 8.1.5 全面武装，打造安全QQ
- 8.2 MSN聊天安全防范
 - 8.2.1 MSN保护盾让聊天更安全
 - 8.2.2 MSN安全中心
- 8.3 电子邮箱攻击与防范
 - 8.3.1 邮箱密码破解方式介绍
 - 8.3.2 社会工程学盗取密码实例解析
 - 8.3.3 邮箱使用口令的安全防范
 - 8.3.4 防范文件编辑器破解Fox mail账户
- 8.4 网络游戏账号防盗
 - 8.4.1 哪些网游账号容易被盗
 - 8.4.2 网游盗号手段分析
 - 8.4.3 网游盗号实例剖析
 - 8.4.4 网游保镖捍卫网游安全

<<电脑硬道理 - 网络攻防>>

8.5 网上银行安全防范

8.5.1 网上银行安全隐患

8.5.2 网上银行安全防护

网络炸弹攻防实例

9.1 网络炸弹概述

9.1.1 什么是网络炸弹

9.1.2 炸弹的分类

9.2 初级炸弹攻防

9.2.1 蓝屏炸弹

9.2.2 Ping轰炸防范

9.2.3 UDP攻击

9.2.4 蜗牛炸弹

9.3 邮件炸弹攻防

9.3.1 初识邮件炸弹

9.3.2 邮件炸弹的危害

9.3.3 邮件炸弹KaBoom实战

9.3.4 防范邮件炸弹

9.4 DoS拒绝服务攻防

9.4.1 DoS攻击原理简述

9.4.2 目标的确定

9.4.3 常见工具介绍

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>