

<<计算机病毒与木马程序剖析>>

图书基本信息

书名：<<计算机病毒与木马程序剖析>>

13位ISBN编号：9787900107589

10位ISBN编号：7900107584

出版时间：2003-12-1

出版时间：北京科海电子出版社

作者：张友生,米安然

页数：378

字数：514000

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>

<<计算机病毒与木马程序剖析>>

内容概要

本书与网络及系统安全紧密相联，通过大量的实例全面地分析了计算机病毒与特洛伊木马所涉及的各种技术和攻击手段，详细地剖析了计算机病毒与特洛伊木马的程序源代码，深入地分析了这些网络攻击的防范和清除技术，让读者真正做到知己知彼，实现防范的目的。

读者通过学习本书，可以对网络安全有较深入的认识，对计算机病毒与特洛伊木马所涉及的各种技术和方法有系统的理解，能够独立完成网络信息安全的管理工作，能够编写网络安全管理程序。

本书理论与实践相结合，适用于广大的软件工程师、网络爱好者、网络程序员、网络管理员、大学计算机软件专业和网络专业的学生，以及从事信息安全工作的人员。

<<计算机病毒与木马程序剖析>>

书籍目录

第1部分 网络安全基础知识

第1章 互联网与信息安全

1.1 网络基本概念

1.1.1 计算机网络的发展

1.1.2 计算机网络的定义

1.1.3 计算机网络的元素

1.1.4 计算机网络的分类

1.2 网络应用协议简介

1.2.1 协议的定义

1.2.2 OSI七层模型

1.2.3 常用的网络协议

1.3 TCP/IP协议分析

1.3.1 协议分层

1.3.2 数据封装

1.3.3 TCP/IP协议的端口号

1.3.4 IP地址

1.3.5 RFC

1.3.6 应用程序编程接口

1.3.7 常用小工具

1.4 Internet服务

1.4.1 WWW服务

1.4.2 E-mail

1.4.3 FTP服务

1.4.4 Telnet服务

1.5 网络信息安全

1.5.1 网络信息安全的定义

1.5.2 网络信息安全的目标

第2章 网络系统安全配置技术

2.1 网络安全的主要因素

2.1.1 网络操作系统本分的安全问题

2.1.2 传输线路的安全问题

2.1.3 网络系统硬件的安全问题

2.1.4 网络系统管理的安全问题

2.2 网络安全的主要措施

2.2.1 完善操作系统

2.2.2 消除电磁辐射

2.2.3 严格身份认证

2.2.4 加强网络安全管理

2.2.5 传输加密、电子签名

2.2.6 采用安全防护技术

2.3 安全评估与安全策略

2.3.1 安全评估的内容

2.3.2 安全策略

2.4 电子邮件系统的安全性

2.5 入侵侦测和漏洞检测技术

<<计算机病毒与木马程序剖析>>

- 2.5.1 入侵侦测
- 2.5.2 漏洞检测
- 2.5.3 入侵侦测和漏洞检测的系统模型
- 2.6 访问控制技术与策略
 - 2.6.1 入网访问控制
 - 2.6.2 网络权限控制
 - 2.6.3 目录级控制
 - 2.6.4 属性控制
- 2.7 动态安全防护体系
 - 2.7.1 网络安全的特征
 - 2.7.2 动态安全防护体系
- 第2部分 计算机病毒
- 第3章 计算机病毒概述
 - 3.1 病毒的定义
 - 3.2 病毒的特征
 - 3.3 病毒的分类
 - 3.4 计算机病毒的发展趋势
- 第4章 病毒编制的关键技术
 - 4.1 引导型病毒编制的关键技术
 - 4.1.1 硬盘主引导程序剖析
 - 4.1.2 硬盘主引导程序剖析
 - 4.1.3 引导型病毒编制技术
 - 4.2 DOS病毒编制的关键技术
 - 4.2.1 COM文件结构及运行原理
 - 4.2.2 EXE文件结构及运行原理
 - 4.2.3 文件型病毒编制技术
 - 4.3 Windows PE文件结构及运行原理
 - 4.4 Windows病毒编制的关键技术
 - 4.5 利用Outlook漏洞编写病毒
 - 4.6 病毒技术新动向
- 第5章 病毒程序源码实例剖析
 - 5.1 CIH病毒源码剖析
 - 5.2 “主页”病毒源码剖析
 - 5.3 “欢乐时光”病毒源码剖析
 - 5.4 “爱虫”病毒源码剖析
 - 5.5 “美丽杀”病毒源码剖析
 - 5.6 “为花谷”网页病毒源码剖析
 - 5.7 “红色代码”病毒源码剖析
 - 5.8 “求职信”病毒源码剖析
- 第6章 病毒攻击的防范与清除
 - 6.1 病毒攻击的防范
 - 6.2 病毒的清除
 - 6.2.1 怎样发现病毒
 - 6.2.2 手工清除病毒
 - 6.3 杀毒软件的编制技术
 - 6.3.1 病毒特征码
 - 6.3.2 查毒程序源码分析

<<计算机病毒与木马程序剖析>>

6.3.3 杀毒程序源码剖析

第3部分 特洛伊木马

第7章 木马的基本概念

7.1 木马的定义

7.2 木马的特征

7.3 木马的功能

7.4 木马的分类

7.5 远程控制、木马与病毒

7.5.1 病毒与木马

7.5.2 黑客与木马

7.5.3 远程控制与木马

7.6 木马的发展方向

7.7 木马实例介绍

7.7.1 NetSpy的运行

7.7.2 NetSpy的功能

第8章 木马常用攻击手段

8.1 修改系统文件

8.1.1 在Win.ini文件中加载

8.1.2 在System.ini文件中加载

8.1.3 文件修改的程序实现

8.2 修改系统注册表

8.2.1 注册表基础知识

8.2.2 有关函数说明

8.2.3 修改注册表的实现方法

8.3 修改文件打开关联

8.4 共享硬盘数据

8.5 远程屏幕抓取

8.5.1 与位图有关的结构体

8.5.2 函数介绍

8.5.3 代码实例分析

8.6 远程关机或重新启动

8.7 键盘与鼠标的控制

8.7.1 鼠标的控制

8.7.2 模拟按键的实现

8.8 远程文件管理

8.8.1 常用FTP函数分析

8.8.2 程序示例

第9章 木马程序开发技术

9.1 Socket的基本概念

9.1.1 Socket的引入

9.1.2 Socket编程的基本概念

9.1.3 Socket的类型

9.2 基本的Socket函数

9.3 Windows系统的Socket编程

9.3.1 使用WinSock API

9.3.2 使用数据报Socket

9.3.3 使用流式Socket

<<计算机病毒与木马程序剖析>>

9.3.4 等待事件

9.4 木马程序的隐藏技术

9.5 程序的自动加载运行技术

9.6 目标机器信息的获取

9.6.1 有关结构体

9.6.2 程序实例

9.7 用户事件的记录

9.8 进程操作技术

第10章 木马攻击的防范与清除

10.1 防范木马的攻击

10.2 木马的清除

<<计算机病毒与木马程序剖析>>

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>