

《Rootkit隐遁攻击技术及其贰

图书基本信息

书名：《Rootkit隐遁攻击技术及其防范》

13位ISBN编号：9787121306182

出版时间：2017-1-1

页数：271

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Rootkit隐遁攻击技术及其贰

内容概要

本书系统论述了Rootkit隐遁攻击的概念、原理、应用技术及检测取证。首先，简要回顾了Rootkit的由来、定义、原理、类型及其演化。其次，阐述了Rootkit技术的基础理论，包括硬件系统、软件系统，以及Windows内核驱动程序设计。然后，重点探讨了Rootkit攻击技术的具体类型及其实现，包括用户层Rootkit、内核层Rootkit、固件Rootkit及硬件Rootkit。最后，从防御的角度讨论了Rootkit检测与取证技术，以及Rootkit未来的发展趋势。本书取材新颖，聚焦前沿，内容丰富，可作为IT和安全专业人士的研究指导用书，同时也适合作为高等学校计算机安全专业本科、研究生的参考教材。

作者简介

第1章Rootkit概述

- 1.1Rootkit的由来
- 1.2Rootkit的定义
- 1.3Rootkit的原理
 - 1.3.1计算机系统的抽象
 - 1.3.2Rootkit设计理念
- 1.4Rootkit的类型及其演化
- 1.5本章小结

第2章硬件系统

- 2.1保护模式概述
- 2.2保护模式执行环境
- 2.3保护模式CPU特权级
- 2.4保护模式内存分段与分页
- 2.5内存访问控制体系
- 2.6本章小结

第3章软件系统

- 3.1Windows系统的设计原则
- 3.2Windows系统的体系结构
- 3.3Windows的分段与分页
- 3.4Windows系统服务调用机制
 - 3.4.1中断分发
 - 3.4.2异常分发
 - 3.4.3系统服务分发
- 3.5本章小结

第4章Windows内核驱动程序

- 4.1概述
- 4.2重要数据结构
 - 4.2.1IRP
 - 4.2.1.1堆栈
 - 4.2.1.2IRP的传递与完成
- 4.3WDM驱动的基本结构
 - 4.3.1DriverEntry
 - 4.3.2AddDevice
 - 4.3.3IRP处理例程
 - 4.3.4Unload
 - 4.3.5内核驱动程序实例
- 4.4本章小结

第5章用户层Rootkit

- 5.1用户层Rootkit概述
- 5.2用户层Rootkit技术
 - 5.2.1IAT钩子
 - 5.2.2InlineFunction钩子
 - 5.2.3DLL注入
 - 5.2.4DLL劫持
- 5.3本章小结

第6章内核层Rootkit

- 6.1内核层Rootkit概述

- 6.2内核层Rootkit技术
 - 6.2.1系统表格钩子
 - 6.2.2映像修改
 - 6.2.3过滤驱动程序
 - 6.2.4直接内核对象操纵 (DKOM)
- 6.3本章小结
- 第7章底层Rootkit
 - 7.1扩展的处理器模式
 - 7.1.1系统管理模式
 - 7.1.2虚拟机技术
 - 7.2固件
 - 7.2.1板载BIOS
 - 7.2.2扩展ROM
 - 7.2.3ACPI组件
 - 7.2.4UEFI组件
 - 7.3硬件
 - 7.4本章小结
- 第8章Rootkit检测与取证分析
 - 8.1Rootkit检测概述
 - 8.2Rootkit检测技术
 - 8.2.1IAT Hook检测示例
 - 8.2.2IRP Hook检测示例
 - 8.2.3IDT Hook检测示例
 - 8.2.4MSR Hook检测示例
 - 8.2.5SSD THook检测示例
 - 8.2.6Inline Hook检测示例
 - 8.2.7基于免疫的Rootkit检测技术
 - 8.3Rootkit检测工具
 - 8.4Rootkit取证分析
 - 8.4.1证据的获取与存储
 - 8.4.2取证分析
 - 8.5Rootkit取证工具
 - 8.5.1磁盘镜像工具
 - 8.5.2内存镜像工具
 - 8.5.3内存分析工具
 - 8.5.4进程转储工具
 - 8.5.5时间轴取证工具
 - 8.5.6证据收集工具
 - 8.5.7电子邮件取证工具
 - 8.5.8大数据取证分析工具
 - 8.6本章小结
- 第9章Rootkit的未来
 - 9.1Rootkit的发展趋势
 - 9.2Rootkit的防御方向
- 参考文献

《Rootkit隐遁攻击技术及其贰

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:www.tushu000.com