

<<Microsoft , UNIX及Ora>>

图书基本信息

书名：<<Microsoft , UNIX及Oracle主机和网络安全>>

13位ISBN编号：9787121000027

10位ISBN编号：7121000024

出版时间：2004-7-1

出版时间：电子工业出版社

作者：Erik Pace Birkholz Foundstone公司,潘吉兵,赵彦玲,董春红

页数：967

字数：967000

译者：潘吉兵,赵彦玲,董春红

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>

## <<Microsoft , UNIX及Ora>>

### 内容概要

本书凝聚了数十位权威的国际安全专家的实战经验和总结。

它不仅提供了Windows系统、UNIX系统和Oracle系统的主机及网络安全解决方案，而且包括了企业的安全管理规范的原则；它既高屋建瓴地描述了企业内部网整体面临的安全威胁和漏洞，又细致地介绍了Windows , UNIX , Oracle及无线LAN等各种系统具体的漏洞，同时还提供了各种漏洞评测方法和补救预防措施。

本书可作为企业安全技术人员实战的好帮手，也适合作为安全技术初学者了解各种漏洞和安全工具的实用指南，更适合做大中院校相关专业和企业安全技术培训的教材。

## 作者简介

Erik Pace Birkholz :

erik@SpecialOpsSecurity.com

Erik Pace Birkholz ( CISSP , MCSE ) 是Foundstone公司的首席咨询师和主讲师。

自1995年以来, Erik已经在世界各地主持了多次内部安全评估、渗透测试、主机安全评测、Web应用程序评估和安全培训。

Erik是全球最

## 书籍目录

第1章 评测内部网的安全性 1.1 概述 1.1.1 为好奇心和精通技术创造机会 1.1.2 漏洞在哪里 1.1.3 DEFCON 1 1.2 确定内部网安全面临的威胁 1.3 内部网安全性的评测策略 1.3.1 枚举业务运营的各个方面 1.3.2 资产盘点 1.3.3 选择范围, 确定优先级别 1.3.4 评测主机和网络的安全漏洞 1.3.5 弥补漏洞 1.4 向管理层提供结果文档 1.5 实施安全“金牌”基准 1.6 安全检查列表 1.7 小结 1.8 站点链接 1.9 解决方案快速追踪 1.10 常见问题第2章 公司资产清单和暴露点 2.1 概述 2.2 进行资产盘点 2.2.1 基本资产盘点的工具和技术 2.3 通过Wardialing来发现公司资产 2.3.1 Wardialing的工具和技巧 2.4 管理资产暴露点 2.4.1 一个需要评测主机暴露点的场景 2.4.2 减少暴露点的建议 2.5 安全检查列表 2.6 小结 2.7 站点链接 2.8 邮件列表 2.9 相关书籍 2.10 解决方案快速追踪 2.11 常见问题第3章 寻找高危漏洞 3.1 概述 3.2 漏洞评测产品的特点 3.3 研究商业漏洞扫描工具 3.4 研究免费漏洞扫描工具 3.5 案例分析: 攻击Windows域 3.6 安全检查列表 3.7 小结 3.8 站点链接 3.9 邮件列表 3.10 相关书籍 3.11 解决方法快速追踪 3.12 常见问题第4章 攻击和防护Windows XP Professional 4.1 概述 4.2 Windows XP的特性 4.3 攻击Windows XP Professional 4.4 攻击XP Professional补充应用程序 4.5 防护XP Professional 4.6 维护XP系统良好的安全性能 4.7 安全检查列表 4.8 小结 4.9 站点链接 4.10 相关论坛和邮件列表 4.11 相关书籍 4.12 解决方案快速追踪 4.13 常见问题第5章 攻击和防护Windows 2000 5.1 概述 5.2 Windows 2000基本特性 5.3 Windows 2000安全要素 5.4 攻击Windows 2000 5.5 防护和加固Windows 2000 5.6 安全检查列表 5.7 小结 5.8 站点链接 5.9 邮件列表 5.10 相关书籍 5.11 解决方案快速追踪 5.12 常见问题第6章 保护活动目录 6.1 概述 6.2 了解活动目录基本特性 6.3 攻击活动目录 6.4 加固活动目录 6.5 安全检查列表 6.6 小结 6.7 站点链接 6.8 邮件列表 6.9 相关书籍 6.10 解决方案快速追踪 6.11 常见问题第7章 保护Exchange和Outlook网络入口 7.1 概述 7.2 Exchange 2000简介 7.3 了解Exchange 2000的基本安全风险 7.4 防止Exchange的安全问题 7.5 审计可能的安全漏洞 7.6 遵循最佳实践经验 7.7 安全检查列表 7.8 小结 7.9 站点链接 7.10 邮件列表 7.11 相关书籍 7.12 解决方案快速追踪 7.13 常见问题第8章 攻击和防护DNS 8.1 概述 8.2 了解DNS机制 8.3 利用DNS漏洞 8.4 保护DNS 8.5 安全安装和配置DNS守护进程 8.6 安全检查列表 8.7 小结 8.8 站点链接 8.9 邮件列表 8.10 相关书籍 8.11 解决方案快速追踪 8.12 常见问题第9章 攻击和防护Microsoft终端服务器 9.1 概述 9.2 终端服务崩溃的原因 9.3 攻击终端服务器 9.4 保护终端服务器 9.5 案例分析: 攻击终端服务器 9.6 安全检查列表 9.7 小结 9.8 站点链接 9.9 邮件列表 9.10 相关书籍 9.11 解决方案快速追踪 9.12 常见问题第10章 保护IIS 10.1 概述 10.2 从过去中学习 10.3 准备操作系统 10.4 确保Web服务安全 10.5 确保Web站点安全 10.6 授权用户 10.7 发布Web内容 10.8 安全检查列表 10.9 小结 10.10 站点链接 10.11 邮件列表 10.12 相关书籍 10.13 解决方案快速追踪 10.14 常见问题第11章 攻击客户Web应用程序 11.1 概述 11.2 使用源代码 11.3 定位可能的交互作用 11.4 查明攻击地址 11.5 执行和检查 11.6 使用自动操作 11.7 安全检查列表 11.8 小结 11.9 站点链接 11.10 邮件列表 11.11 相关书籍 11.12 解决方法快速追踪 11.13 常见问题第12章 攻击和防护Microsoft SQL Server 12.1 概述 12.2 SQL服务器的发展 12.3 了解有关SQL服务器安全的基本问题 12.4 攻击SQL Server 12.5 防守SQL Server 12.6 为SQL Server编写安全的应用程序 12.7 安全检查列表 12.8 小结 12.9 站点链接 12.10 邮件列表 12.11 相关书籍 12.12 解决方法快速追踪 12.13 常见问题第13章 攻击和防护Oracle 13.1 概述 13.2 攻击监听器 13.3 攻击数据库 13.4 攻击Oracle应用服务器 13.5 防护Oracle 13.6 安全检查列表 13.7 小结 13.8 站点链接 13.9 现有安全工具链接 13.10 邮件列表 13.11 相关书籍 13.12 解决方法快速追踪 13.13 常见问题第14章 攻击和防护UNIX 14.1 概述 14.2 攻击UNIX 14.3 策划UNIX系统安全 14.4 特定平台配置 14.5 保护遗留系统 14.6 安全检查列表 14.7 小结 14.8 站点链接 14.9 邮件列表 14.10 相关书籍 14.11 解决方法快速追踪 14.12 常见问题第15章 无线LAN: 发现和防护 15.1 概述 15.2 802.11介绍 15.3 侦测无线网络 15.4 从有线的角度发现802.11网络 15.5 保护无线网络 15.6 侦测802.11攻击 15.7 安全检查列表 15.8 小结 15.9 站点链接 15.10 邮件列表 15.11 相关书籍 15.12 解决方法快速追踪 15.13 常见问题第16章 网络架构第17章 构建人力资源因素第18章 创建高效的企业安全策略

#### 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>