

<<网络安全评估>>

图书基本信息

书名：<<网络安全评估>>

13位ISBN编号：9787508338613

10位ISBN编号：7508338618

出版时间：2006-1

出版时间：中国电力出版社

作者：麦肯兰勃

页数：378

字数：445000

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>

<<网络安全评估>>

内容概要

了解自己所在系统安全性的最好方法是对其进行攻击。

很多管理员只是以很随意的方式对自己所在系统进行一些不严格的测试，而本书则讲述了专业的网络安全分析人员与顾问用来识别和评估计算机网络的步骤。

你将在本书中学到渗透测试人员（通常是政府、军事及商业网络的安全维护人员）所用的工具、窍门以及相应的技术，所有这些将使得你设计与部署的网络能有效地防备恶意的渗透、工具和脚本。

这一透彻的、见解深刻的安全评估指南以对工具的介绍开始，并很快地将你引向黑客为查找那些可以攻陷目标网络的机器所采用的方法和步骤。

本书的主体部分包含了多个章节，这些章节集中介绍了不同的网络组件、运行的不同服务及其被攻击的方式。

每一章以对网络安全人员提出的如何战胜黑客攻击的建议作为结束。

本书中覆盖的主题包括：用于进行网络安全评估的工具的详尽技术资料；测试SSH、DNS与LDAP等常见服务；测试NetBIOS、CIFS与RPC等Microsoft Windows服务；测试运用在Apache与Microsoft IIS上的Web应用程序；评估Oracle、SQL Server与MySQL等数据库服务；评估IPsec、FWZ与PPTP等VPN服务；评估应用程序的风险，包括对堆、栈、整数溢出、格式化字符串bug以及其他相关问题的详尽描述；风险规避信息与策略，包括检查清单。

本书采用了专业安全分析人员与顾问用来识别和评估风险的步骤，并遵循CESG CHECK与NSA IAM等政府标准。

<<网络安全评估>>

书籍目录

序 前言 第一章 网络安全评估 商业利益 IP : Internet的基础 对Internet攻击者的分类 评估服务定义 网络安全评估方法学 循环的评估方法 第二章 需要的工具 操作系统 免费的网络扫描工具 商业化的网络扫描工具 依赖具体协议的评估工具 第三章 Internet主机与网络枚举 Web 搜索引擎 NIC 查询 DNS查询 枚举技术回顾 枚举的应对措施 第四章 IP网络扫描 ICMP探测 TCP端口扫描 UDP 端口扫描 IDS逃避与过滤欺骗 底层IP评估 网络扫描总结 网络扫描的应对措施 第五章 评估远程信息服务 远程信息服务 systat与netstat DNS finger auth SNMP LDAP rwho RPC rusers 远程信息服务的应对措施 第六章 评估Web服务 Web 服务 识别Web服务 识别子系统与组件 研究Web服务漏洞 访问保护机制薄弱的信息 评估CGI脚本和定制的ASP页面 Web 服务攻击应对措施 第七章 评估远程维护服务 远程维护服务 SSH Telnet r-services X Window 微软远程桌面协议 VNC Citrix 远程维护服务攻击的应对措施 第八章 评估FTP与数据库服务第九章 评估Windows网络服务第十章 评估电子邮件服务第十一章 评估IP VPN服务第十二章 评估Unix RPC服务第十三章 应用层风险第十四章 评估方法学应用实例附录一 TCP、UDP端口与ICMP消息类型附录二 漏洞信息源

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>