第一图书网, tushu007.com

<<黑客攻防技术与实践>>

图书基本信息

书名：<<黑客攻防技术与实践>>

13位ISBN编号：9787111267850

10位ISBN编号：7111267850

出版时间：2009-7

出版时间：机械工业出版社

作者：李建华 编

页数：359

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

前言

伴随电子商务、电子政务的全面铺开，信息安全行业面对的将是一场前所未有的机遇和挑战。
由于信息网络的开放性和复杂性，安全保障的各个状态都处于一种不稳定的快速变化过程中。
安全保障的各个环节，如风险评估，威胁监测与分析、事件发现、事件控制甚至系统恢复与生存等，都需要具备足够的动态适应能力，以便适应各种变化的状况。
然而，如何达到这个要求也面临大量的技术挑战。
黑客攻防技术是伴随着Internet的快速延伸而不断发展和完善的技术体系。
本书以信息攻防的一对矛盾体为线索为读者逐一展开黑客技术体系的全貌，分为攻击技术、防御技术、攻防实践三个部分，共18章。
第一部分为黑客攻击技术，涉及九个方面的攻击类型和方法；第二部分为防御技术，包括防火墙、入侵检测系统、数据保护、Microsoft Windows系统安全、Web安全等；第三部分为攻防实践，是上述各种技术的实践环节。
本书的特色在于：同时涉及攻击与防御技术，将各种攻防技术系统化；配有专门的实践部分，强化了攻防理论与具体实践的结合。
本书可用作大专院校计算机、信息安全等专业的本科生、研究生教材，也适合网络安全技术爱好者自学使用。
本书主编是李建华教授，单蓉胜博士参加了第12～15章、18章的编写并负责统稿工作；李昀博士参加了第1-5章、16章的编写工作；陈楠硕士参加了第6-11章、17章的编写工作。
感谢赵旭东博士生对全书的校对。
本书的顺利出版，要感谢上海交通大学信息安全工程学院的领导和老师所给予的大力支持和帮助。
本书作为面向21世纪高等院校信息安全技术的教材，体现了信息安全技术课程改革的方向之一。
本课程建议授课学时为40学时，实验学时为20学时，并要求先修计算机网络课程。
由于编著水平有限，书中难免存在不妥之处，敬请读者批评指正。

内容概要

本书介绍了信息安全攻防技术的基本原理和实现工具。
全书共分18章，既介绍了网络攻击技术，如信息搜集、拒绝服务攻击、网络嗅探、欺骗与会话劫持、Web攻击、密码破解、病毒、蠕虫与木马、后门技术和踪迹隐藏等攻击技术，也详细分析了防火墙、入侵检测技术、数据保护、Windows系统安全、Web安全等技术，还介绍了攻击技术和防御技术的实践操作实例。
　本书既可以作为高等学校信息安全课程的教材，也适合企事业单位的网络管理员、系统管理员等专业技术人员作为工作学习和参考。

书籍目录

出版说明前言第1章　基础知识 1.1　历史上的十大黑客事件 1.2　网络安全问题的产生 1.3 网络安全成为信息时代人类共同面临的挑战 1.4　网络四大攻击方法及发展趋势　1.4.1　网络四大攻击方法　1.4.2　攻击技术发展趋势　1.5　网络安全产品　1.5.1　物理隔离　1.5.2　逻辑隔离　1.5.3　防御来自网络的攻击　1.5.4　防止来自网络上的病毒　1.5.5　反垃圾邮件　1.5.6　身份认证　1.5.7　加密通信和虚拟专用网　1.5.8　公钥相关软件及服务　1.5.9　入侵检测和主动防卫　1.5.10　网管、审计和取证　1.5.11　其他产品 1.6　小结 1.7　习题第2章　攻击方法概述　2.1　与攻击有关的术语　2.2　与网络攻防有关的基础知识　2.2.1 TCP/IP连接端及标记　2.2.2 TCP连接的建立　2.2.3 IP地址　2.2.4 常用DOS命令　2.3　攻击的分类　2.3.1　主动攻击和被动攻击　2.3.2　更常用的分类　2.4　黑客常用的攻击方法及完整的入侵步骤　2.4.1　黑客常用的攻击方法　2.4.2　完整的入侵步骤　2.5　小结　2.6　习题第3章　信息搜集　3.1　信息搜集的意义和步骤　3.2　主机信息搜集　3.2.1　用ping来识别操作系统　3.2.2　通过连接端口返回的信息进行识别　3.2.3　利用rusers和finger搜集用户信息　3.2.4　用host发掘更多信息　3.2.5　利用专门的软件来搜集信息　3.3　Web网站信息搜集　3.3.1 由域名得到网站的IP地址　3.3.2　网站基本信息查询　3.3.3　网站注册信息及地理位置搜集　3.4　网络拓扑结构探测　3.4.1　手工探测目标网络结构　3.4.2　可视化的网络结构探测集成工具　3.5　端口扫描　3.5.1　端口扫描器和安全扫描器　3.5.2　端口扫描技术 3.6　小结 3.7　习题第4章　拒绝服务攻击　4.1　拒绝服务攻击　4.1.1　DoS攻击的网络基础　4.1.2　DoS攻击的原理　4.1.3　典型的DoS攻击　4.2　分布式拒绝服务攻击　4.2.1　分布式拒绝服务攻击的原理　4.2.2　DDoS攻击的危害　4.2.3　典型的DDoS攻击　4.3　分布式反射拒绝服务攻击　4.4　小结　4.5　习题第5章　嗅探 5.1　嗅探器的工作原理　5.1.1　嗅探器概述　……第6章　欺骗与会话劫持第7章　Web攻击第8章　缓冲区溢出攻击　第9章　密码破解攻击第10章　病毒、蠕虫与木马第11章　后门技术和踪迹隐藏第12章　防火墙技术第13章　入侵检测系统第14章　数据保护第15章　Windows系统安全第16章　Web安全第17章　攻击技术实践第18章　防御技术实践参考文献

章节摘录

插图：第1章　基础知识1.1 历史上的十大黑客事件DNA杂志在印度全国软件和服务企业协会（Nasscom）与孟买警方开展互联网安全周活动，并回顾历史上的十大黑客事件时深刻认识到，即使是那些被认为固若金汤的系统在黑客攻击面前也总是显得不堪一击。
20世纪90年代早期，出现了一位在世界范围内举足轻重的黑客——Kevin Mitnick。
诺基亚（Nokia），富士通（Fujitsu），摩托罗拉（Motorola）和Sun Microsystems等世界上几大科技和电信公司的电脑系统都曾被他“光顾”过。
1995年他被FBI逮捕，于2000年获得假释。
他从来不把自己的这种入侵行为称为黑客行为，按照他的解释，应为“社会工程（Social Engineering）”。
2002年11月，伦敦人Gary McKinnon在英国被指控非法侵入美国军方90多个电脑系统。
1995年，来自俄罗斯的黑客Vladimir Levin在互联网上上演了精彩的“偷天换日”。
他是历史上第一个通过入侵银行电脑系统来获利的黑客。
当年，他侵入美国花旗银行并盗走1000万美元。
之后，他把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。
1990年，为了获得在洛杉矶地区kiis-fm电台第102个呼人者的奖励——保时捷944 s2跑车，Kevin Poulsen控制了整个地区的电话系统，以确保他是第102个呼人者。
最终，他如愿以偿地获得了跑车并为此人狱3年。
他现在是Wired News的高级编辑。

编辑推荐

《黑客攻防技术与实践》是由机械工业出版社出版。

第一图书网, tushu007.com

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