

<<网络攻防技术原理与实战>>

图书基本信息

书名：<<网络攻防技术原理与实战>>

13位ISBN编号：9787030124807

10位ISBN编号：7030124804

出版时间：2004-1

出版时间：科学出版社

作者：卿斯汉

页数：303

字数：450000

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>

<<网络攻防技术原理与实战>>

前言

因特网的迅速发展，促进了网络互联、信息共享与信息的全球化。

信息全球化不但为我国带来发展机遇，也向我们提出了严峻的挑战。

多年来，国外的主流操作系统Windows等主宰了IT市场，与此同时，基于Windows操作系统的应用也成为黑客攻击的主要目标。

当前，随着网络互联范围的扩大，信息与网络安全已成为全球关注的问题，从一定意义上讲，没有信息系统的安全，就没有完整的国家安全。

我们应该从战略的高度考虑信息系统的安全，不仅应当重视信息系统的防范，同时应当重视针对网络与主机系统的攻击技术与手段，更好地保护我国基础信息网络和重要信息系统的安全。

以往，我们的科研工作与实际工作大多数以防范为主，近年来，虽然我国有关数据加密、防火墙、入侵检测、备份与恢复、PKI公钥基础设施等的论文、著作、技术报告与工程项目日益增多，但是，专门涉及网络攻防、网络攻与防并重的专著，还不多见。

实际上，网络攻击技术与网络防范技术是密不可分的，二者是相辅相成、相互促进、螺旋式发展的。

因此本书的出版恰逢其时，将会对促进我国信息安全事业的发展起到积极作用。

本书由我国著名信息安全学者卿斯汉研究员领衔编著。

全书共分20章，由网络攻击的历史、现状和发展趋势；网络攻击的目标与分类方法；网络攻击模型；网络攻击身份隐藏实战技术；网络攻击目标系统信息收集实战技术；网络攻击弱点挖掘实战技术；网络攻击目标权限获取实战技术；网络攻击活动隐藏实战技术；网络攻击实施实战技术；网络攻击开辟后门实战技术；网络攻击痕迹清除实战技术；常用的网络攻击关键技术原理剖析；网络重要服务的攻击理论与实践；网络攻击案例；网络攻击的防范策略与体系；防火墙技术原理与应用；弱点检测技术原理与应用；入侵检测技术原理与应用；网络诱骗系统原理与应用；计算机及网络攻击应急响应及取证等章节组成，涵盖了网络攻防领域的主要内容。

本书对网络攻防进行了清晰和完整的描述，不仅深入阐述了网络攻防的技术原理，而且通过大量实例对攻防的技术原理进行佐证，反映出当代网络安全攻防研究发展的趋势。

卿斯汉研究员及其项目组成员，长期从事信息系统安全的基础理论与关键技术研究，在信息安全域有很深的造诣和丰富的实践经验。

本书通过作者的工程实践，包括一些国内外文献中鲜有的技术细节，可以加深读者对网络攻防内涵的理解。

本书内容丰富，取材合理，有理论，有实践，是一部特点鲜明、深入浅出的网络攻防专著。

我衷心祝贺本书的顺利出版，我相信，她的面世将有力地促进我国信息安全事业的发展，并产生广泛影响。

<<网络攻防技术原理与实战>>

内容概要

本书是一本系统论述网络攻防与信息对抗的专著。

书中总结了目前网络攻击现状与发展趋势，详细地分析了计算机及网络系统面临的威胁与黑客攻击方法，详尽、具体地披露了攻击技术的真相，给出了防范策略和技术实现措施。

全书共分20章，主要内容包括：网络攻击的历史、现状和发展趋势，网络攻击的目标与分类方法，网络攻击模型，各种实际攻击技术，常用的网络攻击关键技术原理，网络重要服务的攻击理论与实践，网络攻击案例，网络攻击的规范策略与体系、防火墙技术原理与应用、弱点检测技术原理与应用、入侵检测技术原理与应用、网络诱骗系统原理与应用、计算机及网络攻击应急响应及取证等。

本书可以作为计算机、通信、信息安全专业本科高年级学生、硕士生和博士生的教材，也可供从事网络与网络安全工作（企业IT人员、网络管理和维护人员、网络应用开发者）和有关方面研究工作的广大工程技术人员参考。

<<网络攻防技术原理与实战>>

书籍目录

第1章 网络攻击的历史、现状与发展趋势 1.1 网络安全历史回顾 1.2 网络攻击技术的演变第2章 网络攻击的目标与分类方法 2.1 网络攻击的目标 2.2 网络攻击分类第3章 网络攻击模型 3.1 网络攻击模型描述 3.2 攻击身份和位置隐藏 3.3 目标系统信息收集 3.4 弱点信息挖掘分析 3.5 目标使用权限获取 3.6 攻击行为隐蔽 3.7 攻击实施 3.8 开辟后门 3.9 攻击痕迹清除 3.10 攻击讨论第4章 网络攻击身份隐藏实战技术详解 4.1 IP地址欺骗或盗用 4.2 自由代理服务器 4.3 MAC地址盗用 4.4 电子邮件 4.5 盗用他人网络账户 4.6 干扰技术 4.7 数据加密技术第5章 网络攻击目标系统信息收集实战技术详解 5.1 确定攻击目标 5.2 目标信息搜集的理念 5.3 获取网络信息的工具 5.4 获取目标网络信息的软件第6章 网络攻击弱点挖掘实战技术 6.1 网络攻击弱点挖掘的必要性 6.2 弱点挖掘的基本过程 6.3 常用的弱点挖掘原理与方法 6.4 弱点数据库第7章 网络攻击目标权限获取实战技术详解 7.1 基于社交活动的目标权限获取 7.2 基于网络监听的目标权限获取 7.3 基于网络系统弱点的目标权限获取 7.4 基于网络账号口令破解的目标权限获取 7.5 基于网络欺骗的目标权限获取 7.6 基于TCP会话劫持的目标权限获取第8章 网络攻击活动隐藏实战技术详解 8.1 进程活动隐藏 8.2 文件隐藏 8.3 网络连接隐藏 8.4 网络隐蔽通道第9章 网络攻击实施实战技术详解 9.1 网络可控性攻击实施 9.2 拒绝服务攻击实施 9.3 网络保密性攻击实施 9.4 网络完整性攻击实施 9.5 网络抗抵赖性攻击实施第10章 网络攻击开辟后门实战技术详解第11章 网络攻击良迹清除实战技术详解 11.1 UNIX系统攻击良迹清除基本原理与实例 11.2 Windows NT系统攻击良迹清除基本原理与实例 11.3 防火墙系统攻击痕迹清除基本原理与实例 11.4 入侵检测系统攻击痕迹清除基本原理与实例 11.5 WWW服务攻击痕迹清除基本原理与实例第12章 常用的网络攻击关键技术原理剖析 12.1 口令破解技术原理剖析 12.2 网络嗅探技术原理剖析 12.3 网络端口扫描技术原理剖析 12.4 缓冲区溢出攻击技术原理剖析 12.5 拒绝服务攻击技术原理剖析第13章 网络重要服务的攻击理论与实践 13.1 防火墙系统攻击理论方法与实践 13.2 网络入侵检测系统攻击理论方法与实践第14章 网络攻击案例 14.1 UNIX WWW网站攻击实例 14.2 MS SQL数据库攻击实例第15章 网络攻击的防范策略与体系 15.1 网络攻击防范策略 15.2 常见的网络安全保障体系模型第16章 防火墙的技术原理与应用 16.1 防火墙概述 16.2 防火墙技术 16.3 防火墙的系统结构第17章 弱点检测技术的原理与应用 17.1 弱点检测概述 17.2 弱点检测技术 17.3 弱点扫描器的系统结构、原理和分类 17.4 弱点数据库第18章 入侵检测技术的原理与应用 18.1 入侵检测概述 18.2 入侵检测技术 18.3 入侵检测系统的结构与分类 18.4 常见的入侵检测系统及应用第19章 网络诱骗系统原理与应用 19.1 网络诱骗技术概述 19.2 网络诱骗系统的体系结构 19.3 网络诱骗技术 19.4 常见的网络诱骗工具及产品第20章 计算机及网络攻击应急响应与取证 20.1 计算机及网络攻击应急响应 20.2 计算机及网络攻击取证附录1 常见默认账号与口令附录2 专家们公认最危险的20个安全弱点及防范附录3 网络攻击工具网址主要参考文献

<<网络攻防技术原理与实战>>

章节摘录

插图：网络信息系统的安全问题不仅涉及保密性，而且涉及到完整性、可用性、可控性等多个方面。恶意事件、突发事件、恐怖主义和国家敌对行为等都将影响到信息系统的安全。

2000年发生的以网络瘫痪为目标的黑客攻击事件震惊了全美国，从受攻击的商业网站到各个网络公司，从联邦调查局到司法部，乃至白宫和国会，都受到了巨大的震撼。

受社会政治环境气候影响，重大事件常常触发网络攻击的发生。

黑客们攻击Web网站，修改主页，表明自己的观点，扩大影响。

纵观计算网络发展，网络攻击事件时有发生。

据有关资料统计表明，从事计算机业务的工作人员中，工程人员占70%以上，内部人员占65%左右。同时“白领犯罪”分子占绝大部分，大部分网络安全事件与内部人员相关。

堡垒最容易从内部攻破，如何有效地防止内部人员作案是网络安全急需解决的问题。

网络技术在造福人类的同时，也成为犯罪分子作案的工具。

种种网络安全事件向人们敲响了警钟，网络安全绝不可掉以轻心。

网络安全事关重大，必须努力寻求解决办法。

网络安全在攻击和防御的对抗中，不断向前发展。

<<网络攻防技术原理与实战>>

编辑推荐

《网络攻防技术原理与实战》由科学出版社出版。

<<网络攻防技术原理与实战>>

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>