<<网络攻防技术>>

图书基本信息

书名：<<网络攻防技术>>

13位ISBN编号：9787111276326

10位ISBN编号：7111276329

出版时间：2009-8

出版时间：机械工业出版社

作者：吴灏

页数：230

前言

在信息化高度发展的今天，计算机网络已经把国家的政治、军事、经济、文化教育等行业和部门紧密地联系在一起，成为社会基础设施的重要组成部分。
随着网络技术的发展，网络安全问题日趋严重。
黑客利用网络漏洞对网络进行攻击、传播病毒和木马、控制他人的计算机和网络、篡改网页、破坏网络的正常运行、窃取和破坏计算机上的重要信息，严重影响了网络的健康发展。
网络信息安全已成为事关国家安全、经济发展、社会稳定和军事战争成败的重大战略性课题，在维护国家利益、保障国民经济稳定有序发展、打赢未来战争中占有重要地位。
目前国内已有一批专门从事信息安全基础研究、技术开发与技术服务的研究机构与高科技企业，形成了我国信息安全产业的雏形。
但由于国内信息安全技术人才相对不足，阻碍了我国信息安全事业的发展，为此，国内很多高校开设了信息安全专业，并将“网络攻防技术”作为该专业的一门主要课程。
作为一本专门针对本科生网络安全课程的教材，本书比较详细地介绍了现有的主要攻击手段和方法，剖析了系统存在的缺陷和漏洞，让网络安全防护更有针对性。
在此基础上，对网络防御中常用的技术和方法进行了较为系统的分析和介绍。
通过本课程的学习，学生可以了解和掌握网络攻击的手段和方法，系统掌握网络防御的基本原理和技术，熟悉网络安全管理的相关知识，为将来从事网络安全的研究、安全技术的开发和网络安全管理打下坚实的基础。
本书涉猎面广，不仅突出实用性，而且强调对技术原理的掌握。
限于篇幅，书中没有涉及信息安全的重要支撑技术——密码学，如读者有兴趣，请参阅有关书籍。
本书共分15章，各章的内容既独立又有联系，主要内容如下：第1章介绍网络安全威胁、网络攻击的分类、攻击的五个步骤，并且列出了网络攻击导致的后果，展望了网络攻击技术的主要发展趋势。
第2章从网络信息挖掘、网络扫描技术、网络拓扑探测、系统类型探测四个方面对信息收集技术进行详细的介绍。
第3章从口令的强度、存储和传输三个方面对常见的口令攻击技术和防范方法进行介绍。
第4章介绍了缓冲区溢出的相关概念、类型，详细讨论了溢出利用的基本原理及如何编写Shellcode代码。
第5章介绍恶意代码的现状、危害和发展历程，介绍几种主要的恶意代码类型，并归纳出恶意代码的攻击模型。
在此基础上分析了恶意代码所使用的关键技术，详细阐述了基于主机的恶意代码防范技术和基于网络的恶意代码防范技术。
第6章介绍了Web应用的基本模型和相关概念，详细讨论了对Web应用程序的两种常见的攻击方法，并给出了相应的防范策略。
第7章介绍了嗅探器的原理及嗅探器的实现过程，并列出了一些编写方法，最后介绍了嗅探器的检测与防范方法。
第8章按照TCP／IP协议的层次，对假消息攻击进行分类，并详细介绍每一层对应的攻击技术。
第9章详细地介绍了拒绝服务攻击的概念、成因和原理。
第10章主要探讨了网络安全模型、网络安全的评估标准、安全策略、网络的纵深防御、安全检测、安全响应、灾难恢复和网络安全管理等方面。
第11章介绍了访问控制的原理、模型及实现，详细介绍了操作系统访问控制机制和网络访问控制机制。
第12章重点介绍了目前广泛采用的防火墙技术，包括它们所能提供的安全特性与优缺点。
第13章介绍了与防火墙完全不同的一种网络安全技术——入侵检测，讨论了入侵检测系统的模型、技术，并介绍了几种开源的网络入侵检测软件。
第14章介绍了蜜罐技术的基本概念和技术原理，并详细讨论了两种典型的蜜罐应用实例。
第15章介绍了内网安全管理的内容及目标，并讨论了终端的接入控制、非法外联监控、移动存储介质

等安全管理内容。
本书由解放军信息工程大学信息工程学院网络工程系组织编写，具体分工如下：第1、10章由吴灏编写；第2、3章由曹宇、胡雪丽编写；第4章由魏强编写；第5章由王亚琪编写；第6章由奚琪编写；第7、8章由彭建山编写；第9章由耿俊燕编写；第11章由尹中旭编写；第12、13章由朱俊虎编写；第14章由曾勇军、徐长征编写；第15章由吴濒、邵峥嵘编写。
全书由吴灏教授统稿，胡雪丽协助。
此外，王高尚、曹琰、崔颖、任栋、刘国栋、朱磊、李正也参与了本书的编写工作。
由于网络攻防技术的快速发展，再加之作者水平有限，疏漏和错误之处在所难免，恳请读者和有关专家不吝赐教。

<<网络攻防技术>>

内容概要

本书由浅入深地介绍了网络攻击与防御技术。
首先，从网络安全所面临的不同威胁入手，详细介绍了信息收集、口令攻击、缓冲区溢出、恶意代码、Web应用程序攻击、嗅探、假消息、拒绝服务攻击等多种攻击技术，并给出一定的实例分析，然后，从网络安全、访问控制机制、防火墙技术、入侵检测、蜜罐技术等方面系统介绍网络安全防御技术，进而分析了内网安全管理的技术和手段。
　　本书可作为高等院校网络信息安全课程的教材或者教学参考书，也可作为网络信息安全专业技术人员、网络安全管理人员、网络使用者的一本实用的网络安全工具书。

<<网络攻防技术>>

书籍目录

章节摘录

插图：第1章 网络攻击技术概述网络攻击也称为网络入侵（network intrusion），指的是网络系统内部发生的任何违反安全策略的事件，这些事件可能来自系统外部，也可能来自系统内部；可能是故意的，也可能是无意偶发的。
1.1 网络面临的安全威胁网络安全威胁是网络系统所面临的已发生过的安全事件或潜在的安全事件的负面影响。
网络安全威胁的种类很多，对计算机网络的影响各不相同，产生的原因也各不相同。
网络安全威胁主要来自以下几个方面：1.协议缺陷TCP／IP作为Internet使用的标准协议集，是攻击者实施网络攻击的重点目标。
TCP／IP协议簇是目前使用最为广泛的网络互连协议，但TcP／IP协议簇本身存在着一些安全问题。
TcP／IP协议设计时面向的是封闭、专用的网络环境，首要解决的是网络互连、缺乏认证等基本的安全特性，否则会带来许多安全威胁。
例如，中间人攻击所利用的就是通信双方、网络设备之间没有认证的缺点，即使有中间人插入，通信双方也不会察觉。
TcP／IP协议的缺陷主要表现在：缺乏有效的身份鉴别机制，通信双方无法可靠识别身份；缺乏有效的信息加密机制，通信内容容易被第三方窃取。
2.软件漏洞 在操作系统和应用系统中，由于系统越来越复杂，代码的规模越来越庞大，加之软件开发者开发软件时的疏忽，或者是编程者安全知识的局限，几乎可以肯定地说所有的软件都存在实现的缺陷和漏洞。
几乎所有引起身份被盗、网络中断、数据丢失与网站崩溃的安全破坏都有一个根本的原因，即软件代码本身编写粗糙。

<<网络攻防技术>>

编辑推荐

《网络攻防技术》从网络安全所面临的不同威胁入手，结合网络攻击现状与发展趋势，由浅入深地介绍了网络攻击与防御的方法，向读者揭开“ 黑客 ”的神秘面纱。
首先，详细地介绍了现有的主要攻击手段和方法，剖析了系统存在的缺陷和漏洞，披露了攻击技术的真相。
然后，以此为基础，对网络防御中常用的技术和方法进行了系统的《网络攻防技术》主要特点：侧重理论和技术分析，使读者全面掌握网络攻击的手段和方法以及网络防御的基本原理。
提供大量的范例和图示，供读者借鉴，使读者一目了然。

版权说明