

<<网络攻防原理与实践>>

图书基本信息

书名：<<网络攻防原理与实践>>

13位ISBN编号：9787040341621

10位ISBN编号：704034162X

出版时间：2012-2

出版时间：田俊峰、杜瑞忠、杨晓晖 高等教育出版社 (2012-02出版)

作者：田俊峰 等著

页数：336

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>

<<网络攻防原理与实践>>

内容概要

《高等学校信息安全系列教材：网络攻防原理与实践》全面论述了计算机及网络系统各种攻防手段的基本原理和应用技术，对网络安全的相关概念与技术进行了深入探讨，详尽地分析了信息系统的各种攻击技术及相应的防御措施，并通过提供大量实践例程使读者加深对内容的理解。

全书共分3个部分，共17章，第1部分对网络攻防进行了概述，内容涉及第1章和第2章；第2部分详细描述了网络攻击技术及其原理，内容涉及第3~9章；第3部分分别从密码技术、身份验证、防火墙和蜜罐等技术详细描述了网络防御技术。

《高等学校信息安全系列教材：网络攻防原理与实践》可作为高等学校计算机、通信及信息专业的高年级本科生的教材，也可作为从事计算机科学与技术、网络工程、信息与通信工程等与信息安全有关的科研人员、工程技术人员和技术管理人员的参考用书。

书籍目录

第一部分 网络攻防概述第1章 网络安全概述1.1 网络安全现状1.2 网络安全概念1.3 网络安全目标1.4 影响网络安全的主要因素1.5 网络安全模型1.5.1 PPDR模型1.5.2 APPDRR模型第2章 黑客与黑客攻击2.1 黑客的历史2.2 黑客的动机2.3 黑客攻击的步骤2.3.1 攻击前奏2.3.2 攻击实施2.3.3 巩固控制2.4 黑客攻击发展趋势第二部分 网络攻击第3章 目标系统信息收集技术3.1 信息收集概述3.2 网络信息挖掘3.3 网络扫描技术3.4 网络拓扑探测3.5 操作系统类型探测3.5.1 主动探测技术3.5.2 被动探测技术第4章 漏洞扫描技术4.1 漏洞的概念4.2 漏洞的分类4.3 漏洞扫描4.3.1 漏洞扫描简介4.3.2 漏洞扫描的实现方法4.4 漏洞库及其使用4.5 常用的漏洞扫描工具第5章 缓冲区溢出攻击5.1 缓冲区溢出攻击概述5.1.1 缓冲区溢出攻击原理5.1.2 缓冲区溢出攻击历史5.2 缓冲区溢出类型5.2.1 缓冲区溢出分类5.2.2 系统内部处理缓冲区的机制5.2.3 基于栈的缓冲区溢出5.2.4 基于堆的缓冲区溢出5.2.5 基于非初始化数据段的缓冲区溢出5.3 缓冲区溢出利用技术5.3.1 缓冲区溢出攻击的基本条件5.3.2 溢出点定位5.3.3 覆盖执行控制地址5.3.4 跳转地址的确定5.3.5 ShellCode的定位5.4 ShellCode编写5.4.1 ShellCode简介5.4.2 Windows下的函数调用原理5.4.3 查看函数地址5.4.4 汇编代码的编写和机器码的生成 ShellCode5.5 缓冲区溢出攻击的防范5.5.1 系统管理上的防范5.5.2 软件开发过程中的防范策略第6章 网络欺骗攻击6.1 IP欺骗攻击原理与防范6.1.1 IP欺骗原理6.1.2 IP欺骗过程6.1.3 IP欺骗的防范方法6.2 ARP欺骗攻击原理与防范6.2.1 ARP协议6.2.2 ARP数据包格式6.2.3 ARP协议的工作过程6.2.4 ARP缓存污染6.2.5 ARP欺骗的实现6.2.6 ARP攻击的检测与防范6.3 DNS欺骗攻击原理与防范6.3.1 DNS简介6.3.2 DNS解析过程6.3.3 DNS欺骗6.3.4 DNS欺骗原理6.3.5 DNS报文格式6.3.6 对DNS欺骗攻击的防御6.4 ICMP重定向攻击与防范6.4.1 ICMP重定向6.4.2 ICMP重定向工作方式6.4.3 ICMP重定向攻击6.4.4 ICMP重定向攻击防范6.5 网络钓鱼6.5.1 网络钓鱼概述6.5.2 网络钓鱼的防御第7章 Web应用安全攻击7.1 Web应用安全概述7.2 SQL注入攻击原理与防范7.2.1 SQL注入攻击的概念7.2.2 SQL注入漏洞的判断7.2.3 判断后台数据库类型7.2.4 发现Web虚拟目录7.2.5 确定XP_CMDSHLL可执行情况7.2.6 上传木马7.2.7 获取系统管理员权限7.2.8 SQL攻击的防范7.3 跨站脚本攻击7.3.1 跨站脚本攻击的定义7.3.2 跨站脚本攻击的原理7.3.3 跨站脚本攻击的实现过程7.3.4 跨站脚本攻击的检测与防范7.4 基于会话状态的攻击7.4.1 相关概念7.4.2 会话攻击原理7.4.3 针对会话状态攻击的防范7.5 Web攻击的防范第8章 拒绝服务攻击8.1 拒绝服务攻击概述8.1.1 拒绝服务攻击的概念8.1.2 拒绝服务攻击的动机8.1.3 拒绝服务攻击的分类8.2 分布式拒绝服务攻击8.2.1 DIMS攻击的基本原理8.2.2 DDoS攻击的典型过程8.3 常见的DoS/DDoS攻击方式8.3.1 SYN Flood攻击8.3.2 ACK Flood攻击8.3.3 UDP Flood攻击8.3.4 ICNPFlood攻击8.3.5 Connection Flood攻击8.3.6 HTTPCet攻击8.3.7 UDIPDNSQuery Flood攻击8.3.8 DoS/DDoS工具分析8.3.9 傀儡网络8.4 拒绝服务攻击的防范8.4.1 拒绝服务攻击的发展趋势8.4.2 拒绝服务攻击的防御8.4.3 拒绝服务攻击的检测第9章 恶意代码9.1 恶意代码概述9.1.1 恶意代码的发展史9.1.2 恶意代码的分类9.1.3 恶意代码的危害及传播趋势9.2 计算机病毒9.2.1 计算机病毒的概念9.2.2 计算机病毒的结构9.2.3 计算机病毒的特点9.2.4 计算机病毒的分类9.2.5 计算机病毒的防范9.3 特洛伊木马9.3.1 特洛伊木马概述9.3.2 木马的结构和原理9.3.3 木马隐藏技术9.3.4 木马的分类9.3.5 木马植入手段9.3.6 木马的特点9.3.7 木马的防范技术9.4 蠕虫9.4.1 蠕虫概述9.4.2 蠕虫的结构和原理9.4.3 蠕虫的特点9.4.4 蠕虫的防范技术9.4.5 病毒、木马、蠕虫的区别第3部分 网络防御参考文献

<<网络攻防原理与实践>>

章节摘录

版权页:第1章 网络安全概述以Internet为代表的全球性信息化浪潮日益高涨,计算机以及信息网络的应川日益普及,应川层次正在深入,应川领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展,典型的有政府部门业务系统、金融业务系统、企业商务系统等,网络已经深刻地影响着社会的政治、经济、文化、军事、意识形态和社会生活等各个方面。

伴随网络的普及,网络安全日益成为影响网络效能的重要问题,针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量仍在持续不断地增加,网络攻击与入侵行为对国家安全、经济和社会生活造成了极大的威胁。

而由于网络自身所具有的开放性、自由性等特点,在增加应用自由度的同时,对安全提出了更高的要求。

因此,网络安全已成为世界各国当今共同关注的焦点。

<<网络攻防原理与实践>>

编辑推荐

《高等学校信息安全系列教材：网络攻防原理与实践》全面论述了计算机及网络系统各种攻防手段的基本原理和应用技术，理论与实践相结合，有利于读者在短时间内全面了解网络攻防技术，同时也为读者提供了一个进一步深入学习的通道。

<<网络攻防原理与实践>>

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>