<<网络安全编程技术与实例>>

图书基本信息

书名：<<网络安全编程技术与实例>>

13位ISBN编号：9787111246169

10位ISBN编号：7111246160

出版时间：2008-8

出版时间：机械工业出版社

作者：刘文涛

页数：387

前言

随着计算机网络的飞速发展，安全问题日益突出。
为了保护网络安全，一些网络安全技术应运而生，对网络安全技术的研究也变得至关重要。
网络安全是一门实践性很强的学科。
理论联系实际，实践出真知，本书就是在这个背景下产生的，以实例为指导，以编程为中心，旨在让读者对网络安全相关技术有更深的理解。
本书主要对网络安全方面的一些技术进行了案例分析，通过编程实现了一些常用的网络安全技术，包括网络安全扫描、网络协议分析、网络数据包生成和网络入侵检测。
本书不是讲解网络安全理论的书籍，关于网络安全理论的书籍市面上很多，读者可以参考很多经典作品。
本书主要讲解关于网络安全的编程技术，对常用网络安全技术进行了编程实现。
由于网络安全涉及的内容很多，本书主要对网络安全扫描、网络协议分析、网络数据包生成和网络入侵检测进行了编程实现。
其他的网络安全内容，限于篇幅没有涉及。
第l章介绍了一些网络安全方面的基本知识。
第2章主要介绍了一些基本的网络安全编程，包括Winsock套接字编程，还涉及进程、计时器以及注册表编程等。
在Winsock套接字编程中主要介绍了套接字编程的基本原理，以及基于流式套接字和基于数据报套接字的编程方法。
重点介绍了原始套接字的基本原理，对其发送数据包和接收数据包的过程进行了分析。
在本章还介绍了获取网络接口的编程方法，此功能在网络安全编程中经常要用到。
第3章对网络安全扫描进行了编程实现，首先简单阐述了一些网络安全扫描的知识，其中包括各种端口扫描、隐秘扫描、漏洞扫描、远程操作系统识别、服务器扫描、木马扫描等技术。
然后通过实例程序对每种网络安全扫描技术进行了编程实现，其中涉及Winsock原始套接字编程技术以及多线程技术等。
在端口扫描中实现了TCP扫描，包括17CP连接扫描、TCP sYN扫描以及TCP FIN扫描等。
还实现了ICMP扫描、了UDP扫描、多线程扫描技术等。
对服务器扫描实现了’Web服务器扫描、FTP服务器扫描以及Email服务器扫描。
第4章讲述网络协议分析系统的实现过程，使用编程工具Visual C++6.0介绍了多种协议分析实现方法，包括使用Winsock原始套接字方法以及WinPcap方法。
本章详细阐述了网络协议分析系统的实现原理，包括数据包捕获技术、协议分析技术。
介绍了利用Winsock原始套接字捕获网络数据包的过程，列举了利用Winsock原始套接字方法对IP协议分析、TCP协议分析、LJDP协议分析以及ICMP协议分析的编程案例。
最后利用WinPcap方法实现了一个基于MFC的协议分析系统，实现了对以太网、ARP、IP、TCP、LIDP、ICMP协议的分析功能，是一个内容比较综合的网络协议分析系统实例。
第5章介绍网络数据包生成编程技术，阐述了几种生成网络数据包的方法，包括Winsock原始套接字方法，WinPcap生成数据包的方法以及使用L,ibnet生成数据包的方法。
介绍了使用这些方法生成数据包的基本过程以及它们的区别，并且列举了利用这些方法分别实现常用协议数据包的生成实例，具体包括以太网数据包生产、ARP数据包生成、IP数据包生成、LIDP数据包生成、TCP数据包生成和ICMP数据包生成。

<<网络安全编程技术与实例>>

内容概要

本书详细讲述了重要的网络安全技术原理，并进行了编程实现，涉及的技术有网络安全扫描、网络协议分析、网络数据包生成、网络入侵检测。
全书使用Visual C++编程，程序实例丰富，讲解透彻，源代码注释清晰，容易理解。
读者可在www.cmpbook.com下载源代码。
本书供网络安全研究和开发人员以及网络安全爱好者阅读，也可以作为计算机网络和网络安全专业方面的教学参考书。

<<网络安全编程技术与实例>>

书籍目录

章节摘录

第1章 网络安全概述1.1 网络安全原理1.1.1 信息安全根据国际标准化委员会的定义，计算机信息安全是指“为数据处理系统采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。
信息安全要保证信息的保密性、完整性、可用性和可控性。
保密性是指保证信息不被非授权用户使用。
完整性是指保障信息的准确性和完全性，保证信息在存储或传输过程中不被篡改。
可用性是指确保信息为授权用户所正常使用，信息能够按照某种权限按需存取。
可控性是指使用的信息能够被监控，对信息的传输及内容具有控制能力。
由于信息具有抽象性和可变性等特征，使得它在处理、存储和传输的过程中很容易被干扰、滥用和泄露，甚至被窃取、篡改和破坏，所以在实际使用中，信息经常处在不安全的状态。
信息系统不安全的因素主要有物理因素、网络因素、系统因素、应用因素和管理因素等。

版权说明