HZ BOOKS
华章教育

高等院校计算机教材系列

计算机网络安全原理与实现

刘海燕 主编

为教师提供电子课件

机械工业出版社
China Machine Press

高等院校计算机教材系列

计算机网络安全原理与实现

刘海燕 主编
荆涛 王子强 金龙 参编
蔡红柳 王维锋 霍景河

机械工业出版社
China Machine Press

本书系统阐述计算机网络安全的基本原理、技术和方法，包括网络安全基础、网络安全中的攻击技术以及网络安全中的防护技术三大部分。第一篇主要介绍网络协议以及网络攻防编程的基础知识；第二篇主要介绍网络攻击的概念、目标和分类以及攻击的原理及防范方法，并介绍恶意软件技术；第三篇主要介绍网络安全体系结构以及加密技术、认证技术、访问控制、防火墙技术、入侵检测技术等。

本书取材新颖，概念清晰，既可以作为高等院校相关专业本科生、研究生的教学用书，也是网络安全防护人员、网络安全产品开发人员和网络对抗研究人员的参考资料。

图书在版编目（CIP）数据

计算机网络安全原理与实现 / 刘海燕等编著. —北京：机械工业出版社，2009.1
（高等院校计算机教材系列）

ISBN 978-7-111-24531-5

Ⅰ. 计… Ⅱ. 刘… Ⅲ. 计算机网络－安全技术－高等学校－教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2008）第152588号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：朱　劼
北京慧美印刷有限公司印刷·新华书店北京发行所发行
2009年1月第1版第1次印刷
184mm×260mm · 18.75印张
标准书号：ISBN 978-7-111-24531-5
定价：34.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：（010）68326294

前　言

随着信息化的发展，网络已经渗透到社会的各个领域，对科学、技术、政治、经济、军事乃至人类的生活都产生了巨大的影响。网络已经成为人类社会的一项关键基础设施，发挥着至关重要的作用。然而，由于网络规模的不断扩大，网络复杂性随之增强，网络安全问题日益凸显，已经成为阻碍网络应用普及的一个关键要素。

本书围绕“网络攻击和防护技术”这一核心问题展开，重点介绍网络攻击和防护技术的原理，并通过简单示例分析技术的实现。全书分为网络安全基础、网络安全中的攻击技术、网络安全中的防护技术三个部分。

第一篇包括第1～3章，目的是补充读者在网络协议、网络攻防编程方面的基础知识。第1章回顾网络协议的内容，重点强调协议中与攻击和防护有关的部分。UNIX/Linux和Windows是计算机使用的两类主流平台。第2章介绍UNIX/Linux平台上的网络程序设计基础知识，包括编写TCP/UDP程序、原始套接字的使用、使用libpcap捕获数据包、使用libnet构造数据包等知识。第3章介绍Windows平台上的攻防编程，分别介绍Windows下的TCP/UDP编程、原始套接字的使用以及如何操作注册表。

第二篇包括第4～6章，内容涵盖网络攻击的概念、原理和方法。第4章概述网络攻击的发展历史、概念、目标和分类，介绍攻击的基本步骤以及发展趋势。第5章介绍常用的几种攻击技术。对每种技术，按照先介绍相关的概念和原理，接着分析其实现技术并给出演示性的示例，最后介绍如何进行防范的顺序组织内容。通过该章的学习，可以加深对网络攻击技术的理解，掌握相关的防范措施。第6章介绍恶意软件技术，包括病毒技术、蠕虫技术和木马技术，对于每种技术都说明其一般性原理，并给出一些简单的示例。通过这些示例，读者可以加深对恶意软件工作原理的理解，提高防范能力。

第三篇包括第7～12章，内容涉及防护的总体概念以及一些常用的防护技术。第7章介绍安全体系和安全模型的概念以及有关的安全评估标准。第8章介绍密码学，包括对称密钥密码算法、非对称密钥密码算法以及单向散列函数，还将介绍PGP软件的安装和使用；第9章介绍身份认证的概念和主要的认证技术；第10章介绍访问控制策略及其实现机制；第11章介绍防火墙的有关概念和实现技术；第12章介绍入侵检测的原理和实现技术。对每种技术，力求讲清其工作原理，介绍常用工具的使用方法并给出实现示例。

本书既是作者多年来从事教学一线工作经验的总结，也是近年来信息安全技术和网络对抗技术发展的最新成果的体现。由于作者水平有限、时间仓促，加之网络攻防技术发展迅猛，新的知识、原理和技术层出不穷，书中难免存在一些缺点和错误，恳请广大读者不吝赐教，批评指正。

作者

2008年7月

教学建议

教学内容	学习要点及教学要求参考	课时安排参考			可选实验参考内容
		第一层次	第二层次	第三层次	
第1章 网络协议安全基础	• 了解OSI参考模型的7层结构以及各层的功能 • 掌握TCP/IP协议族的四层结构，以及各层的功能 • 掌握链路层的基本概念和以太网帧的结构，理解硬件地址的概念 • 掌握IP地址的分类、理解私用IP和公用IP的概念，了解IP包的结构，理解ARP协议的工作原理，了解RARP协议的作用 • 掌握TCP连接建立过程以及TCP首部的数据格式，了解可能存在的安全问题 • 了解主要的应用层协议的功能和存在的潜在安全问题	2（根据学生对网络原理了解的情况选讲）	2	2	
第2章 UNIX / Linux下的网络程序设计	• 了解套接字的概念和相关结构定义 • 掌握TCP协议的主要套接字函数，掌握基本的TCP协议程序的编写 • 掌握UDP协议的主要套接字函数，掌握简单的UDP协议程序的编写 • 了解原始套接字编程的功能和原理，理解简单的原始套接字编程的步骤和方法 • 了解libpcap函数库的功能和基于libpcap的网络程序的编写步骤和方法 • 了解libnet函数库的功能，了解基于libnet的数据包构造程序的编写步骤和方法	2~4（根据学生对网络编程知识的了解情况选讲）	4~6	6~8	编写基于TCP/UDP协议的网络程序
第3章 Windows攻防编程	• 了解Windows平台上socket编程的基础知识 • 掌握Winsock API的基本函数 • 掌握基于socket API的TCP和UDP编程的步骤和方法 • 了解Windows 原始套接编程的步骤和方法 • 了解Windows注册表的结构和功能 • 掌握操作注册表的主要函数和方法	2（根据学生对网络编程、注册表编程知识的了解情况选讲）	2~4	4	注册表编程实验

（续）

教学内容	学习要点及教学要求参考	课时安排参考			可选实验参考内容
		第一层次	第二层次	第三层次	
第4章　网络攻击的概念与发展	• 了解网络攻击与信息安全的简单发展过程以及国际国内对信息安全事件进行处理的机构 • 了解网络攻击的目标和分类 • 了解网络攻击的一般过程和步骤，以及使用的一般手段和工具 • 了解网络攻击的发展趋势	2	2	2	
第5章　网络攻击技术原理	• 理解网络欺骗的概念，理解IP欺骗、邮件欺骗、Web欺骗、社会工程的形式和基本原理，了解网络欺骗的防范措施 • 理解嗅探的基本原理和实现形式，了解嗅探的防范措施 • 了解网络扫描的基本形式和基本原理，了解扫描工具的使用和功能，了解扫描的防范方法 • 理解口令破解的形式和基本原理，了解口令破解的防范方法，掌握口令管理技术 • 了解系统对缓冲区的管理方法，理解缓冲区溢出原理，了解缓冲区溢出的形式，理解缓冲区溢出的防范方法 • 理解拒绝服务攻击和分布式拒绝服务攻击的原理，了解拒绝服务攻击的一些防范方法	4（根据课程对攻击技术的要求选讲）	4	6～8	UNIX系统口令的字典破解实验、端口扫描、SYN洪泛实验
第6章　恶意软件技术原理	• 理解恶意软件的特点 • 了解病毒的定义、组成结构、特点 • 了解病毒的工作原理以及病毒的预防和检测方法 • 了解蠕虫的工作原理以及检测和预防方法 • 了解木马的实现机制、工作原理、检测防范方法 • 了解恶意软件的发展趋势	2（根据课程对恶意软件的要求选讲）	2	4	脚本编程实验

（续）

教学内容	学习要点及教学要求参考	课时安排参考			可选实验参考内容
		第一层次	第二层次	第三层次	
第7章　安全体系结构与安全模型	• 了解OSI安全体系结构的组成和内容 • 了解TCP/IP安全体系的内容 • 了解几种典型的安全模型 • 了解TCSEC的内容 • 了解CC的内容 • 了解我国计算机安全等级划分与相关标准	2	2	2	
第8章　密码学	• 掌握密码学的相关概念 • 理解密码学的分类 • 了解网络通信中的加密技术、密码的破译以及密码算法的安全性概念 • 理解简单密码算法：替换密码、易位密码、一次一密算法的基本原理 • 掌握对称加密算法DES的基本原理和实现方法 • 理解3DES算法的原理 • 理解RSA算法的基本原理 • 掌握单向散列函数MD5的原理和实现 • 理解消息认证的原理和实现方法 • 理解数字签名的基本原理和实现方法 • 了解PGP软件的功能和使用	4～6（根据课程对密码学的概念、算法、应用的要求选讲）	6	6	• DES算法实验 • MD5算法实验 • PGP软件的使用
第9章　身份认证技术	• 掌握身份认证的基本概念和基本形式 • 理解简单的口令认证的特点 • 了解质询/响应认证、一次性口令认证、双因素认证的基本原理和实现 • 了解RADIUS协议的工作过程 • 理解Kerberos认证协议 • 了解PKI体系的基本内容和基本功能，理解基于PKI的身份认证的基本原理	2	4	4	

（续）

教学内容	学习要点及教学要求参考	课时安排参考			可选实验参考内容
		第一层次	第二层次	第三层次	
第10章 访问控制	• 掌握访问控制的基本概念 • 掌握自主访问控制模型、强制访问控制模型、基于角色的访问控制模型的基本原理和内容 • 掌握访问控制列表、访问控制矩阵、访问控制能力列表的内容和功能 • 理解网络中访问控制的形式和实现手段	2	2	2	
第11章 防火墙技术	• 理解防火墙的基本概念 • 掌握几种防火墙技术，包括包过滤防火墙、应用层代理、电路级网关、NAT的基本原理，以及各自的优缺点 • 理解防火墙的基本功能 • 了解CCProxy、squid代理的功能和基本的使用方法 • 了解netfilter的基本组成和功能 • 了解使用iptables构建防火墙的基本步骤和方法	4～6（根据对防火墙的概念原理、工具使用、防火墙构建的要求选讲）	6～8	6～8	使用iptables命令操作系统的包过滤规则
第12章 入侵检测技术	• 理解入侵检测的概念和作用 • 理解Denning的入侵检测通用模型和CIDF通用入侵检测框架的组成和各部分的功能 • 了解入侵检测系统的分类以及不同种类的入侵检测系统的特点 • 了解入侵检测系统的部署方法 • 理解误用检测方法、异常检测方法的原理 • 了解入侵检测系统面临的挑战和前景 • 了解Snort的安装、使用、配置和规则的撰写 • 了解入侵检测系统的实现技术	4～6（根据对入侵检测的概念原理、工具使用、实现技术的要求选讲）	4～6	4～6	winpcap编程实验
教学总学时建议		32～40	40～48	48～60	10～16

说明：

① 本书可作为信息类本科专业“网络安全”或“网络攻防”课程的教材。本书可满足三个层次的教学需求，第一个层次：目标是掌握网络安全的一般概念和原理、了解基本的管理和使用。第二个层次：掌握网络安全的一般概念和原理、了解基本工具的使用、掌握安全防护工具的实现技术和方法。第三个层次是在第二个层次的基础上，对网络攻击的原理和方

法进行深入学习。这三个层次的教学学时建议如下：

- 对第一个层次，建议学时为32～40。
- 对第二个层次，建议学时为40～48。
- 对第三个层次，建议学时为48～56。

建议学时中包括理论讲解、习题课、课堂讨论以及课内实验所需的学时，实验内容可以从建议的实验中选择几个作为课内实验，其他内容可作为课外实验，由学生在课后完成。不同专业可根据不同的教学要求和计划教学时数酌情对教材内容进行适当取舍。

② 非信息类本科专业使用本书可适当降低教学要求。

③ 若某些信息类本科专业和非信息类本科专业计划教学时数少于建议学时，可以舍去部分章节和相关实现部分的内容，或者降低某些章节的教学要求。

目　录

第二篇　网络安全中的攻击技术

第三篇　网络安全中的防护技术

第一篇　网络安全基础

随着网络应用的普及，网络攻击和防护进入了人们的视野。网络对抗不仅成为政治、经济、国防领域的一种新的对抗形式，而且关系到普通的网络用户。这对了解网络安全、掌握网络攻防技术提出了更高的要求。

本篇的主要目的是补充读者在网络协议、网络攻防编程方面的基础知识，以便理解和掌握后续章节中要介绍的网络攻防技术。第1章将介绍OSI参考模型、TCP/IP协议族，目的是使读者掌握协议的工作原理，熟悉协议所使用的数据结构和可能存在的安全问题。UNIX/Linux和Windows是计算机使用的两类主要平台，攻防技术的设计与开发大多基于这两类平台。第2章将介绍UNIX/Linux平台上的网络编程基础，第3章介绍Windows平台上的攻防编程。与一般的网络程序设计不同，这两章将重点介绍构造攻击程序和进行安全防护所需要的编程技术。

了解攻防程序设计是理解和掌握网络攻击和防护技术的基础，要熟练掌握还需要多下工夫认真研究，希望本篇介绍的内容能够激发大家学习的兴趣，掌握网络攻防的基本知识。

第 1 章　网络协议安全基础

将分布在不同地理位置上的具有独立功能的多台计算机、终端及其附属设备，用通信媒体连接起来，加上网络管理软件后，就构成了计算机网络。最简单的网络就是将两台计算机连接起来，共享文件和打印机及其他共享设备。因特网（Internet）是最复杂的网络，它把分布在全球的各种计算机连接在一起。

无论是网络攻击还是防护，都需要掌握网络连接所使用的协议。本章的目的是使读者掌握协议的工作原理，熟悉协议所使用的数据结构，为后续章节的学习打下基础。

1.1　计算机网络的体系结构

计算机网络是一个非常复杂的系统。两个计算机系统必须高度协调才能相互通信。为了设计复杂的计算机网络，人们采取“分层”的思想，将庞大而复杂的问题转化为若干较小的局部问题，而这些较小的局部问题便于处理和解决，这就是网络的分层体系结构的基本思想。

为了便于实现不同体系结构的网络间的通信和信息交换，国际标准化组织（ISO）制定了一个描述网络通信所需要的全部功能的总框架，即开放系统互联参考模型（Open System Interconnection Reference Model，OSI/RM）。

1.1.1　OSI参考模型

OSI参考模型采用具有七个层次的体系结构，自下而上分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，每层实现相对独立的功能，并通过接口为上层提供服务，如图1-1所示。在逻辑上，每一层都可以看做与其他机器上的相同层之间相互工作，它们之间的通信规则称为协议。

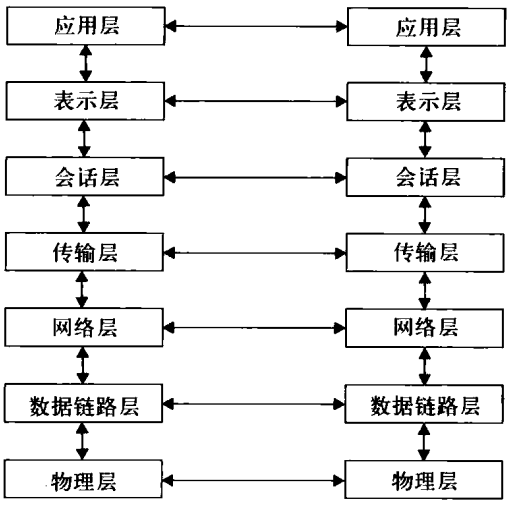

图1-1　OSI参考模型

（1）物理层（physical layer）

这一层负责在两个相邻节点间透明地传输比特流，它为在物理媒体上传输的位流建立规则，定义电缆如何连接到网卡上，用何种传送技术在电缆上发送数据，同时还定义了位同步及检查。这一层的协议数据单元为比特，工作在物理层的设备有集线器（hub）、中继器、放大器等。

（2）数据链路层（data link layer）

所谓链路就是一条点到点的物理线路段，中间没有任何其他的交换结点。在进行数据通信时，两个计算机之间的通路往往是由许多链路串接而成的。数据链路层的任务就是将网络层交下来的数据组装成帧，在两个相邻结点间的链路上无差错地传送以帧为单位的数据。每一帧包括数据和必要的控制信息。控制信息使接收端能够知道一个帧从哪个比特开始、到哪个比特结束，同时检测收到的帧中有无差错。如果发现差错，数据链路层就会放弃出错的帧，然后采取下面两种处理措施之一：或者不作任何处理，或者通知对方重传这一帧，直到正确无误地收到此帧为止。数据链路层可以把一条有可能出差错的实际链路转变成

让网络层向下看起来好像是一条不出差错的链路。

(3) 网络层 (network layer)

计算机网络中的两个计算机之间要进行通信，可能要经过许多个结点和链路，还可能要经过由若干个路由器互联的通信子网。网络层的任务就是要为每台计算机编址，选择合适的路由，使发送站的传输层所传输的分组能够正确无误地按照地址找到目的站，并交付给目的站的传输层。网络层数据的传送单位是分组或包 (packet)。如果包太大，则可能被分片，然后在目的结点进行重组。网络层协议有IP、IPX等，网络层设备包括路由器、包过滤防火墙等。

集线器、交换机、路由器等都是重要的网络互联设备，表1-1给出了这些互联设备的特征与区别。

表1-1 互联设备比较

设备	所在层次	工作特点
集线器、中继器	物理层	共享方式，在一个端口向另外一个端口发送信息的时候，其他端口就不能再有信息传输，连接的所有设备属于一个冲突域
网桥、交换机	数据链路层	根据MAC地址寻址，通过站表选择转发的接口，站表的建立和维护由交换机自动进行，转发速度高。不同接口属于不同冲突域，但属于同一个广播域
路由器	网络层	可以连接异种网络，使用专门的软件协议，根据IP地址进行子网划分和选路，支持多个广播域

(4) 传输层 (transport layer)

这一层的任务是根据下面的通信子网的特性最佳地利用网络资源，并以可靠和经济的方式为两个主机上的进程之间建立一条运输连接，透明地传送报文 (message)。报文是传输层的传送单位，当报文较长时，要先把它分割成若干个分组，然后再交给下一层进行传输。

(5) 会话层

会话层不参与具体的数据传输，它对数据传输进行管理。它在两个互相通信的进程之间建立、组织和协调其交互方式。例如，确定是双工工作还是半双工工作。

(6) 表示层

表示层主要解决用户信息的语法表示问题。表示层将欲交换的数据从适合于某一用户的抽象语法变换为适合OSI系统内部使用的传送语法。

(7) 应用层

这一层是用户的应用程序访问网络服务的地方，它负责整个网络应用程序的工作，如电子邮件、数据库等都利用应用层传送信息。

当两台计算机通过网络通信时，一台机器上的任何一层的软件都假定是在和另一台机器上的同一层进行通信。例如，一台机器上的传输层和另一台机器的传输层通信。第一台机器上的传输层并不关心实际上是如何先通过该机器的较低层，再通过物理媒体和第二台机器的较低层来实现通信的。

1.1.2 TCP/IP体系结构

OSI的目标是使全世界的计算机网络都遵循OSI标准进行互连和交换数据。但是，直到20世纪90年代，OSI参考模型只获得了一些理论研究成果，市场化方面却失败了。现在规模最大、覆盖全世界的Internet并没有使用OSI标准，而是使用TCP/IP (Transmission Control Protocol/Internet Protocol) 体系结构。TCP/IP是事实上的国际标准，许多计算机网络厂商推出的产品都支持TCP/IP。

TCP/IP是一个四层的体系结构，其层次的划分和OSI参考模型不同，如图1-2所示。

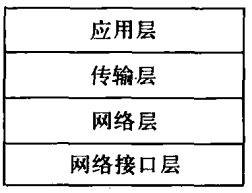

图1-2 TCP/IP体系结构

（1）网络接口层

这一层是该协议的最低层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。其作用是从网络层接收数据包，把数据包进一步处理成数据帧，通过特定的网络设备进行传输，或者从网络上接收数据帧，解开数据帧，抽出数据包交给网络层。该层相当于OSI模型的物理层加上数据链路层。

（2）网络层

这一层有时也称作互联网层。它负责将信息从一台主机传送到指定接收的另一台主机。在TCP/IP协议族中，网络层协议包括IP协议（网际协议）、ARP/RARP（Address Resolution Protocol，地址解析协议；Reverse Address Resolution Protocol，反向地址解析协议）、ICMP协议（Internet Control Message Protocol，Internet控制报文协议），以及IGMP协议（Internet Group Management Protocol，Internet组管理协议）。

（3）传输层

传输层主要为两台主机上的应用程序提供端到端的通信。在TCP/IP协议族中，传输层包括TCP（传输控制协议）和UDP（用户数据报协议）两个协议。TCP为两台主机提供可靠和高效的数据通信，UDP则提供无连接、不可靠的传输服务。

（4）应用层

应用层负责处理特定的应用程序细节。TCP/IP提供一组常用的应用层协议，例如，电子邮件协议、文件传输协议、远程登录协议、超文本传输协议等。除了这些熟知的应用层协议外，用户也可以通过编程建立自己的应用程序。

TCP/IP是一个协议族，包含了100多个协议。其中，TCP和IP是最基本、最重要的两个协议，也最广为人知。在实际中，通常用TCP/IP来表示整个Internet协议族。TCP/IP协议族是一组不同层次上的协议的组合，其各协议之间的层次关系可以用图1-3表示。

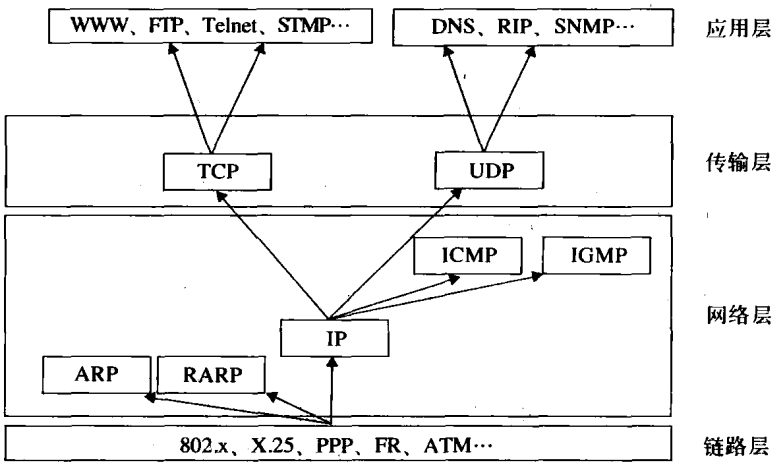

图1-3　TCP/IP协议族各协议间的层次关系

1.2　TCP/IP协议族

在TCP/IP协议族中，所有协议数据单元（PDU）都可以分为首部和本体。首部包括与该层相关的控制信息，而本体是从上一层传下来的数据。每一层把上一层的数据作为本体，再加上本层适当的控制信息作为首部，然后交给下一层处理。下面详细介绍各层常用协议的数据结构和功能。