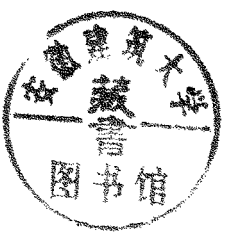
计算机网络技术与网络安全

吴晓刚◎著

光明日报出版社

计算机网络技术与网络安全

吴晓刚 著



光明日报出版社

图书在版编目（CIP）数据

计算机网络技术与网络安全 / 吴晓刚著 . -- 北京 :
光明日报出版社 , 2016.9
ISBN 978-7-5194-1495-5

Ⅰ . ①计… Ⅱ . ①吴… Ⅲ . ①计算机网络 - 安全技术
Ⅳ . ① TP393.08

中国版本图书馆 CIP 数据核字 (2016) 第 178781 号

计算机网络技术与网络安全
著　　者：吴晓刚
责任编辑：李娟　　总 策 划：中国出书网
出 版 人：江亮　　责任校对：邓贝
封面设计：海星传媒　　责任印刷：曹净
出版发行：光明日报出版社
地　　址：北京市东城区珠市口东大街 5 号，100062
电　　话：010-67022197（咨询），67078870（发行）
　　67078235（邮购）
传　　真：010-67078227，6078255
网　　址：http://book.gmv.cn
E-mail：gmcbs@gmw.cn　lijuan@gmw.cn
法律顾问：北京德恒律师事务所龚柳方律师
印　　刷：武汉市楚风印刷有限公司
装　　订：武汉市楚风印刷有限公司
本书如有破损、缺页、装订错误，请与本社联系调换
开　　本：145 × 210　1/32
字　　数：120 千字　　印 张：5.375
版　　次：2016 年 9 月第 1 版　印 次：2016 年 9 月第 1 次印刷
书　　号：ISBN 978-7-5194-1495-5
定　　价：35.00 元

前言

A Brief Introduction

对于计算机网络技术与网络安全这一已经融入现代人生活方方面面的问题，不管是专业计算机科学领域还是日常工作和生活中都备受关注，而且相应的图书也林林总总，不一而足。但是一向都是两个平行的走向，专业的研究专对专业的人群，而通俗易懂的计算机网络技术或者网络安全大多都是傻瓜式的“投机取巧”，相应的方式解决对应的问题，不可能有与之相对应的联系整个技术与网络的宏观问题，也就不会有举一反三的效果。鉴于此，本书以专业的知识，通俗的写法，不但从原理、发展过程，还从实现步骤做全面简单的阐述，并且还在每一个主题下做一个实例训练，力求主题更加清晰，对实际的学习和应用提供有价值的借鉴和参考。

目 录

第1章 引言……**1**
1.1 研究的背景……1
1.2 研究的意义……1
1.3 研究目的……2
1.4 计算机网络技术的概述……3
1.4.1 计算机网络技术的发展与现状……4
1.4.2 计算机网络的组成……6
1.4.3 计算机网络的分类……6
第2章 计算机网络技术的基础与网络结构……**9**
2.1 互联网的基本概述……9
2.2 利用连接器互连……9
2.3 利用互联网互连……11
2.4 网络体系的基本结构……12
2.4.1 OSI 参考模型……12
2.4.2 OSI 模型基本概述……12
2.4.3 服务……14
2.4.4 服务原语……17
2.5 网络协议模型……18
2.5.1 协议分层……18
2.5.2 TCP/IP 协议模型……23
2.5.3 TCP/IP 与 OSI 的关系……24
2.6 以太网技术……25
2.6.1 以太网的概念与原理……25
2.6.2 以太网地址和帧格式……28
2.6.3 嗅探器……33
2.7 TCP/IP协议……36

2.7.1 TCP/IP 协议基础……36
2.7.2 ARP 协议……38
2.7.3 IP 协议……39
2.7.4 ICMP 协议……41
2.7.5 UDP 协议……42
2.7.6 TCP 协议……43
2.8 实训一 常用的网络测试工具的使用……44
2.8.1 使用设置和查看网络接口的工具 ipconfig……44
2.8.2 使用显示网络状态的工具 Netstat……45
2.8.3 使用 测试网络连通状态的工具Ping……46
2.8.4 使用显示经过网关的工具 Tracert……47
2.8.5 如何使用 Sniffer……48
第 3 章 Windows 操作系统和常用服务器配置……50
3.1 Windows 7 操作系统……50
3.1.1 Windows 7 系统的简介……50
3.1.2 管理计算机名、用户、用户组……50
3.1.3 本地安全设置……51
3.1.4 管理文件与文件夹……55
3.2 DNS服务……55
3.2.1 DNS 概述……55
3.2.2 DNS 客户端……56
3.2.3 架设DNS服务器……56
3.2.4 DNS 协议与实例分析……57
3.3 Web服务……58
3.3.1 Web 概述……58
3.3.2 Web 客户端……58
3.3.3 架设Web服务器……59
3.3.4 HTTP 协议和实例分析……59

3.5 FTP 服务……60
3.5.1 FTP 概述……60
3.5.2 FTP 客户端……61
3.5.3 架设 FTP 服务器……61
3.5.4 SMTP 协议、POP3 协议和实例分析……63
3.6 实训二 基于 Windows7 系统服务器架设与配置……63
3.6.1 实训目的……63
3.6.2 实训基础与原理……64
3.6.3 Windows7 操作系统服务器与配置的实训步骤…64
第 4 章 Linux 操作系统和常用服务器配置……66
4.1 Linux 操作系统基础……66
4.1.1 Linux 简介……66
4.1.2 使用 Linux 命令行……66
4.1.3 常用命令……67
4.1.4 文件和目录基础……68
4.1.5 vi 编辑器……72
4.1.6 管理用户和组……72
4.1.7 文件和目录的属性……73
4.1.8 文件打包和压缩……74
4.1.9 使用 grep 进行文本搜索……74
4.1.10 使用 RPM 软件包……75
4.1.11 网络配置……76
4.2 配置 DNS 服务器……76
4.2.1 安装 DNS 服务器……76
4.2.2 安装缓存域名服务器……76
4.2.3 配置主 DNS 服务器……77
4.2.4 重新启动 DNS 服务器……78
4.2.5 配置 DNS 客户端……78

4.2.6 使用 nslookup 命令测试 DNS 服务……79
4.3 配置 FTP 服务器……80
4.3.1 安装 vsftpd 服务器……80
4.3.2 测试 vsftpd 服务器的默认配置……82
4.3.3 配置 vsftpd 服务器，允许匿名用户上传文件……82
4.3.4 配置 vsftpd 服务器的虚拟用户……82
4.4 配置 Web 服务器……85
4.4.1 安装 Apache 服务器……85
4.4.2 测试 Apache 服务器……85
4.4.3 配置 Apache 服务器……85
4.5 配置 E-mail 服务器……89
4.5.1 配置 DNS 服务器……89
4.5.2 安装 Postfix 服务器……90
4.5.3 切换邮件服务器……90
4.5.4 修改配置文件 /etc/postfix/main cf，配置 Postfix 服务器……91
4.5.5 配置 dovecot 服务器，实现 POP 和 IMAP 邮件服务……91
4.5.6 配置电子邮件客户端……91
4.6 实训三 Linux 系统下服务器安装与配置……92
4.6.1 Linux 系统下 DNS 服务器的安装与配置……92
4.6.2 Linux 系统下 vsftpd 服务器的安装与配置……92
4.6.3 Linux 系统下 Web 服务器的安装与配置……93
4.6.4 Linux 系统下 Postfix 服务器的安装与 E-mail 服务器配置……94
第 5 章 信息与网络安全概述……95
5.1 信息安全……95
5.1.1 信息安全概述……95

5.1.2 信息安全的目标……95
5.2 网络安全……96
5.2.1 网络安全概述……96
5.2.2 网络安全典型问题……96
5.2.3 安全体系的构成……98
5.3 安全目标……99
5.4 实训四 网络安全的综合评价……100
5.4.1 评价方式与过程……100
5.4.2 网络安全评估体系……102
5.4.3 网络安全的评判与计算……102
第6章 安全威胁分析……105
6.1 网络与信息安全威胁……105
6.2 漏洞介绍……106
6.2.1 操作系统漏洞……106
6.2.2 传输层与通信层漏洞……107
6.2.3 I立用程序漏洞……108
6.3 网络服务威胁……110
6.3.1 拒绝服务攻击……110
6.3.2 分布式拒绝服务攻击……111
6.4 数据威胁……111
6.4.1 网络监听……111
6.4.2 密码破解技术……112
6.4.3 数据库攻击……112
6.5 实训五 常用网络攻击与防御技术……114
6.5.1 口令破解与防御技术实践……114
6.5.2 假冒网站分析……115
6.5.3 SQL注入攻击及防御实践……116
第7章 安全防御技术分……119

7.1 补丁技术……119
7.2 病毒防护技术……119
7.2.1 计算机病毒的定义与分类……119
7.2.2 各种病毒技术的发展……120
7.2.3 病毒检测的方法……121
7.2.4 计算机病毒的防止策略……122
7.3 加密技术与加密算法……124
7.3.1 密钥与密钥管理……124
7.3.2 密码学与算法……124
7.4 数字签名与数字证书……125
7.4.1 数字签名……125
7.4.2 数字证书……126
7.5 实训六 数字证书 PKI 原理及应用……126
7.5.1 数字证书 PKI 的原理……126
7.5.2 数字证书在安全 PORM 表单中的实际应用…126
7.5.3 数字证书在时间戳服务系统中的实际应用……127
第8章 局域网安全攻防解决方……130
8.1 扫描器……130
8.2 欺骗攻击及防御……130
8.2.1 ARP 欺骗概述……130
8.2.2 ARP 欺骗分析……130
8.2.3 ARP 欺骗防御……131
8.2.4 M·AC 地址欺骗……132
8.2.5 实训——MAC-Port 绑定……133
8.2.6 路由欺骗……134
8.2.7 实训——配置路由协议……135
8.3 Flooding 攻击及防御……139
8.3.1 MAC 洪泛……139

8.3.2 UDP 洪泛……140
8.4 协议攻击……140
8.4.1 生成树攻击……140
8.4.2 DHCP攻击……140
8.4.3 ICMP 攻击……141
8.5 监听攻击与防御……141
8.5.1 PPPoEPAP认证监听攻击……141
8.5.2 MSN 监听攻击……142
8.6 木马……143
8.6.1 木马简介……143
8.6.2 木马原理……143
8.6.3 实训七木马攻击与防范……144
第9章 网络边界流量控制及侵入防御技术……148
9.1 过滤 IP 网络流量……148
9.1.1 路由器 IP 标准 ACL……148
9.1.2 路由器 IP 扩展 ACL……149
9.1.3 实训配置路由器 IP 标准 ACL……149
9.1.4 实训配置路桥 IP 扩展 ACL……149
9.1.5 配置路由器 IPACL 的要点……151
9.2 过滤 Web 和应用流量……151
9.3 流量控制理论及方法……152
9.3.1 P2P 应用及危害防御……152
9.3.2 QQ 特定数据包危害与防御……153
9.4 边界入侵防御技术……154
9.4.1 入侵防御系统……154
9.4.2 数据审计和取证……154
9.4.3 网络安全审计产品的分类……154
9.4.4 实训八 防火墙技术及应用……155

第 10 章 总结与展望……158
10.1 总结……158
10.2 展望……159
参考文献 ……160

第1章 引言

1.1 研究的背景

在世界科技发展史上，几乎每隔100年就会有一项新发明出现，如18世纪的机械时代、19世纪的蒸汽机时代、20世纪的信息时代以及21世纪的大数据时代。

人类从20世纪开始进入信息时代，1946年在冯·诺依曼理论的基础上，第一台计算机诞生美国，它标志着人类社会又向前迈进了崭新一步，信息产业崛起的势头飞速发展。而在信息产业的发展中，有一种技术无限放大了信息社会的生产力，它被称为“计算机网络技术”。

1.2 研究的意义

自人类进入信息社会以来，一些有目的性的组织或个人，对网络环境进行大肆破坏，导致有价值的信息遭到泄露、破坏、侵权等，更有甚者，通过网络对国家政治进行颠覆与干扰，严重威胁到国家、社会、以及个人的合法权益。

由于全社会广泛参与对网络的运用，在此情况与发展趋势下，对网络控制权的管理自然无法得到统一，这样是无法避免的问题。受人们利益、目标、价值分歧性的影响，使信息资源的保护和管理出现脱节和真空，导致计算机网络安全问题变得广泛而复杂。

建设安全的计算机网络对国家、单位、个人有重要的价值和意义：

①防止不法分子破坏国家、单位、个人的荣誉。

②防止资料被篡改，避免对国家、单位、个人造成难以挽回的损失和恶劣影响。

③保护硬件系统不受破坏，避免丢失重要文件。

④避免给国家和社会造成重大经济损失。

⑤防止黑客对页面进行篡改或丑化，传播不健康信息、散布谣言、发表反动言论等，给国家法律和政治、企业与个人形象造成严重的不良后果。

⑥保护机密信息不被窃取和泄露。

⑦防止技术泄露和侵权行为，给国家、单位、个人造成重大损失。

总之，网络安全威胁的存在是个必然，一切归根于网络环境的多变性、复杂性以及信息系统的脆弱性。首先，建设安全的计算机网络，解决的最大的问题是国家经济发展、社会发展和国家安全。网络时代引发了国家的金融安全、经济安全，同时也涉及国家的国防安全、文化安全和政治安全等多方面问题。其次，网络安全建设关系到企业和个人信息安全的问题。企业的商业机密、财产信息、专利技术，个人的隐私、财产、合法权益等，在信息社会受到了严重的威胁。因此，只有保障计算机网络安全，国家、单位、个人的信息安全才能得到保障。

1.3 研究目的

网络等于将全世界的计算机联在了一起，在实现资源开放与共享的同时，信息的安全性也受到了严重的影响。为了防止或避免因为信息泄露造成损失，衍生了以网络技术为根本的网络安全。

网络安全是指运用网络技术建设的安全系统，保证有效的控制介入，保证数据安全的进行传输。研究计算机网络技术与网络安全具体有三个方面目的：

（1）教学方面

通过学习计算机网络技术与网络安全，学生了解计算机网络技术与网络安全的发展与现状，熟知网络的基本机构和原理，更好的掌握计算机网络硬件配置，从网络技术与网络安全的基础开始逐渐深入，全面掌握相关攻防技术。

（2）科研方面

任何科学研究的目标都是创新，而创新的前提就是对基础了解的程度，以及温故知新的态度。计算机网络安全技术也是如此，不断对基础知识的分析、不断对系统流程的推理、不断对技术的研究，或许会得到一些有价值的启示。

（3）个人方面

生活在信息时代的每个人，都应该具有自我保护个人信息安全的意识。通过阅读和学习计算机网络技术与网络安全，不仅可以拓展个人知识面，还可以提高自身网络安全技术能力，防止或避免个人的合法权益受到侵害。

总之，对计算机网络技术与网络安全的研究意义重大，关系到小至个人、大到国家的利益与安全。对计算机网络技术与安全的研究是为了个人和国家营造一个良好的网络环境，使互联网更好地为人们服务。

1.4 计算机网络技术的概述

通信技术结合计算技术形成了计算机网络技术。按照网络协议，集合全球每一台计算机，并将其互相连接，被称为计算机网络。电缆、双绞线、光纤、微波、或通信卫士是连接的介质。计算机网络通过独有对资源集中处理及管理和维护的能力，实现共享硬件、软件和数据资源的功能。

计算机网络包括计算机和网络两部分。其中计算机又称

电子计算机，俗称电脑，是一种能够按照程序运行，自动、高速处理海量数据的现代化智能电子设备。由硬件和软件所组成，没有安装任何软件的计算机称为裸机。常见的形式有台式计算机、笔记本计算机、大型计算机等，较先进的计算机有生物计算机、光子计算机、量子计算机等。而网络就是用物理链路将各个孤立的工作站或主机相连在一起，组成数据链路，从而达到资源共享和通信的目的。所以计算机网络是指将地理位置不同的多台自治计算机系统及其外部网络通过通信介质互联，在网络操作系统和网络管理软件及通信协议的管理和协调下，实现资源共享和信息传递的系统。

1.4.1 计算机网络技术的发展与现状

过去的三百年中，每一个世纪都有一种技术占据主要的地位。18 世纪伴随着工业革命而来的是伟大的机械时代，蒸汽机时代19世纪的关键技术是信息的获取、存储、传送、处理和利用。计算机是 20 世纪人类最伟大的发明之一，它的产生标志着人类开始迈向一个崭新的信息社会，新的信息产业正以强劲的势头迅速崛起。因此，为了提高信息社会的生产力，提供一种全社会的、经济的、快速的存取信息的手段是十分必要的，这种手段是由计算机网络来实现的。

计算机网络的发展大体经历了三个阶段。在 60 年代初期，出现了多重线路控制器。它可以和多个远程终端相连接，构成面向终端的计算机通信网。这种最简单的计算机网络称为第一代计算机网络。

在第一代计算机网络中，计算机是网络的控制中心，终端围绕着中心分布在各处，从而将单一计算机系统的各种资源分散到了每个用户手中。但这种网络系统存在着一些缺点，如果计算机的负荷较重，会导致系统响应时间过长而且单机系统的

可靠性一般较低，一旦计算机发生故障，将导致整个网络系统的瘫痪。

为了克服第一代计算机网络的缺点，提高网络的可靠性和可用性，人们开始研究将多台计算机相互连接的方法。

1969 年 12 月，darpa 的计算机分组交换网 arpanet 投入运行，标志着计算机网络的发展进入了一个新纪元。这个时候的电脑，主机的终端构成了用户资源子网。用户不仅共享通信子网的资源，而且还可共享用户资源之间的丰富的硬件和软件资源。这种以通信子网为中心的计算机网络通常被称为第二代计算机网络。

在第二代计算机网络中，多台计算机通过通信子网构成一个有机的整体，在这种系统中，即使单机出现故障也不会导致整个网络系统全面瘫痪。但是，网络中相互通信的计算机必须高度协调工作，而这种协调是相当复杂的。为了降低网络设计的复杂性，提出了层次模型。

分层设计方法可将大而复杂的问题转化为若干较小易于处理的子问题，使得一个公司所生产的各种机器和网络设备可以非常容易地被连接起来。

但是，在初期各个公司都各自研究开发自己的网络体系结构，而它们的网络体系结构是各不相同的。这种自行发展的网络，由于网络体系结构上差别很大，以至于它们之间互不相容，难于相互连接以构成更大的网络系统。为了使不同公司之间的网络能够互连互通。国际标准化组织提出了一个使各种计算机能够互连的标准框架——开放式系统互连参考模型，简称 osi。osi 参考模型的出现，意味着计算机网络发展到了第三代。

在 osi 参考模型推出后，网络发展道路一直走标准化道路，而网络标准化的最大体现就是 internet 的飞速发展。Internet 遵循 tcp/ip 参考模型，由于 tcp/ip 仍然使用分层模型，因此 internet