高等学校计算机科学与技术教材

计算机网络安全教程

石志国 薛为民 江 俐 编著

清华大学出版社
http://www.tup.tsinghua.edu.cn
北京交通大学出版社
http://press.bjtu.edu.cn

高等学校计算机科学与技术教材

计算机网络安全教程

石志国　薛为民　江　俐　编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书对计算机网络安全技术作了系统的介绍，最大特色是：将安全理论、安全工具与安全编程三方面内容有机结合在一起。三方面内容均来自课堂实践：安全理论来自高校网络安全的课堂讲稿，安全工具来自网络安全国际认证（Certified Internet Webmaster，CIW）的课堂案例，安全编程来自C++/VC++编程（网络安全方向）的课堂案例。精选网络安全方面40多个经典工具和30多个完整源代码，突出实用性、可操作性和连贯性。

全书从网络安全体系上分成四部分。第一部分：计算机网络安全基础，介绍网络安全的基本概念、实验环境配置、网络协议基础及网络安全编程基础。第二部分：网络安全的攻击技术，详细介绍攻击技术“五部曲”——隐藏IP；踩点扫描；获得系统或管理员权限；种植后门；在网络中隐身。第三部分：网络安全之防御技术，介绍Windows操作系统的安全配置方案、加密与解密技术的应用、防火墙及入侵检测技术。第四部分：网络安全综合解决方案，从工程的角度介绍网络安全工程方案的编写。

本书提供教学大纲、全套课程幻灯片、攻防案例的演示动画和源代码，可以从http://press.bjtu.edu.cn或http://www.gettop.net下载。

图书在版编目（CIP）数据

计算机网络安全教程/石志国，薛为民，江俐编著 .—北京：清华大学出版社；北京交通大学出版社，2004.2
（高等学校计算机科学与技术教材）
ISBN 7-81082-249-7

Ⅰ.计… Ⅱ.①石… ②薛… ③江… 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（2003）第124273号

责任编辑：谭文芳
出 版 者：清华大学出版社　邮编：100084　电话：010-62776969
　　北京交通大学出版社　邮编：100044　电话：010-51686045，62237564
印 刷 者：北京东光印刷厂
发 行 者：新华书店总店北京发行所
开　本：787×1 092　1/16　印张：18.75 字数：476千字
版　次：2004年2月第1版　2004年2月第1次印刷
印　数：1～5 000册　定价：27.00元

前　言

网络安全（Network Security）是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。总体上，网络安全可以分成两大方面：网络攻击技术和网络防御技术。只有全面把握两方面的内容，才能真正掌握计算机网络安全技术。

“理论联系实际，并有所发展”是本书的指导方针。

(1)“理论”即计算机网络及网络安全的理论。

(2)“实际”即众多的网络安全攻防工具。

(3)“发展”即利用编程技术编写一些网络安全工具。

全书从三个角度介绍计算机网络安全技术：计算机网络和网络安全理论、网络攻防工具和网络安全编程，包括40多个完整攻防案例和30多个完整源程序。三方面内容均来自实际的工程及课堂的实践，并通过网络安全攻防体系结合在一起。

(1) 网络安全理论选自高校网络安全课堂实践，介绍TCP/IP协议族、网络服务、操作系统安全配置、密码学、防火墙、入侵检测技术和网络安全整体方案的编写。

(2) 网络安全工具选自网络安全国际认证（Certified Internet Webmaster，CIW）的部分案例，介绍经典攻防工具：暴力破解工具、网络扫描工具、木马工具、跳板工具、隐身工具、监听工具、恢复工具、防火墙工具和入侵检测工具，等等。

(3) 网络安全编程选自网络安全方面及其计算机网络的编程案例。所有程序均采用C/C++语言编写，并在VC++6.0环境下调试通过。介绍安全编程核心技术，包括多线程编程、驻留编程、注册表编程、Socket编程、Shell编程、定时器编程及入侵检测编程等。

从网络安全攻防体系上，全书分成4部分，共10章。

第一部分：计算机网络安全基础

第1章网络安全概述与环境配置。介绍网络安全的研究体系、研究网络安全的意义、评价网络安全的标准，以及实验环境的配置。

第2章网络安全协议基础。介绍OSI参考模型和TCP/IP协议族，实际分析IP，TCP，UDP，ICMP协议的结构及其工作原理、网络服务和网络命令。

第3章网络安全编程基础。介绍网络安全编程的基础知识、C语言发展的4个阶段及网络安全编程的常用技术，如Socket编程、注册表编程、驻留编程等。

第二部分：网络安全的攻击技术

第4章网络扫描与网络监听。介绍黑客及黑客攻击的基本概念、如何利用工具实现网络踩点、网络扫描和网络监听。

第5章网络入侵。介绍常用的网络入侵技术，如社会工程学攻击、物理攻击、暴力攻击、漏洞攻击、缓冲区溢出攻击等。

第6章网络后门与网络隐身。介绍网络后门和木马的基本概念，并利用4种方法实现网

络后门。介绍利用工具实现网络跳板和网络隐身。

第三部分：网络安全的防御技术

第7章操作系统安全配置方案。介绍UNIX，Linux和Windows的特点，着重介绍Windows操作系统的安全配置方案：初级配置方案、中级配置方案和高级配置方案。

第8章密码学与信息加密。介绍密码学的基本概念，DES加密算法的概念及如何利用程序实现，RSA加密算法的概念及实现算法，PGP加密的原理和实现。

第9章防火墙与入侵检测。介绍防火墙的基本概念、分类、实现模型，以及如何利用软件实现防火墙的规则集。介绍入侵检测系统的概念、原理，以及如何利用程序实现简单的入侵系统。

第四部分：网络安全综合解决方案

第10章网络安全方案设计。从网络安全工程的角度介绍网络安全方案编写的注意点及评价标准。

由于时间和作者水平有限，难免出现错误，对于本书的任何问题请使用E-mail发送到作者邮箱shizhiguo@tom.com，本书的支持信息将在http://www.gettop.net上发布。

在编写过程中，得到众多老师的指导和帮助。首先感谢两位合作者：北京联合大学的薛为民博士和美国Louisiana State University的江俐博士，与他们愉快的合作使本书能顺利完成。

在网络安全理论方面，感谢北京大学计算机科学技术研究所王选院士、陈晓鸥教授、潘爱民副教授和吴於茜副教授，清华大学计算机系林闯教授，北京科技大学王志良教授、刘冀伟副教授，感谢他们给本书提供了详尽的理论指导。

在网络安全工具方面，感谢新东方IT教育高显嵩老师、金悦老师和栗松涛老师，中国软件行业协会邱钦伦高级工程师，感谢他们为本书提供了丰富的攻防软件工具。

在网络安全编程方面，感谢北京大学计算机科学技术研究所王学武老师和曾建平老师，中央广播电视大学徐孝凯教授、崔林副教授和王春风副教授，中科院软件所李志斌副研究员，感谢他们为本书提供了大量并且详尽的编程资料，并为本书解决了很多编程方面的问题。

感谢众多的学生们，他们的每一个问题，都是本书要强调并解决的知识点，他们的笑容是我最大的动力，本书献给他们，献给最广大的读者。

石志国

2004年2月于北京大学

目　录

第一部分　计算机网络安全基础

第二部分 网络安全的攻击技术

第四部分 网络安全综合解决方案

第一部分

计算机网络安全基础

第 1 章　网络安全概述与环境配置

本章要点

本章介绍网络安全研究的体系、研究网络安全的必要性、研究网络安全的社会意义，目前与计算机网络安全有关的法规，以及如何评价一个系统或者应用软件的安全等级。为了能顺利完成本书介绍的各种实验，本章最后较为详细地介绍实验环境的配置。

1.1　网络安全的攻防研究体系

网络安全（Network Security）是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。

1.1.1　网络安全的攻防体系

从系统安全的角度可以把网络安全的研究内容分成两大体系：攻击和防御。该体系研究内容如图 1-1 所示。

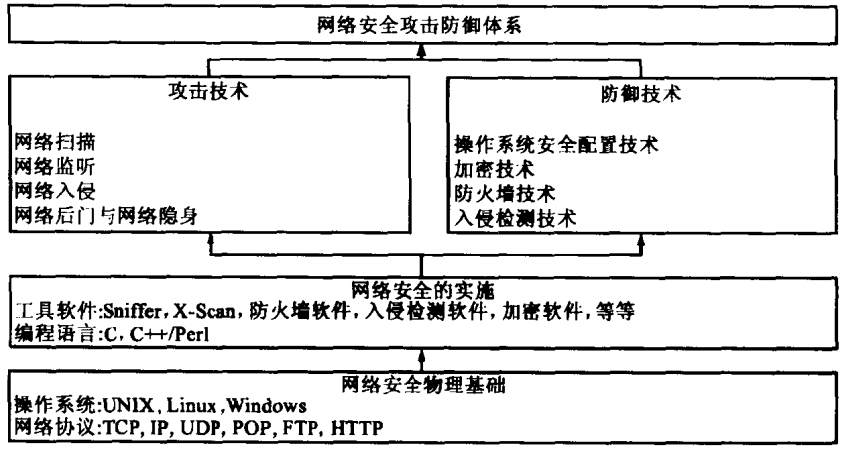

图 1-1　网络安全的体系

如果不知道如何攻击，再好的防守也是经不住考验的，攻击技术主要包括以下 5 个方面。

（1）网络监听：自己不主动去攻击别人，而是在计算机上设置一个程序去监听目标计算机与其他计算机通信的数据。

（2）网络扫描：利用程序去扫描目标计算机开放的端口等，目的是发现漏洞，为入侵该计算机做准备。

（3）网络入侵：当探测发现对方存在漏洞后，入侵到目标计算机获取信息。

（4）网络后门：成功入侵目标计算机后，为了实现对“战利品”的长期控制，在目标计算机中种植木马等后门。

（5）网络隐身：入侵完毕退出目标计算机后，将自己入侵的痕迹清除，从而防止被对方管理员发现。

防御技术包括以下 4 个方面。

（1）操作系统的安全配置：操作系统的安全是整个网络安全的关键。

（2）加密技术：为了防止被监听和数据被盗取，将所有的数据进行加密。

（3）防火墙技术：利用防火墙，对传输的数据进行限制，从而防止被入侵。

（4）入侵检测：如果网络防线最终被攻破，需要及时发出被入侵的警报。

为了保证网络的安全，在软件方面可以有两种选择，一种是使用已经成熟的工具，比如抓数据包软件 Sniffer，网络扫描工具 X-Scan，等等；另一种是自己编制程序，目前常用的网络安全编程语言为 C，C++或者 Perl 语言。

为了使用工具和编制程序，必须熟悉两方面的知识，一方面是两大主流的操作系统：UNIX 家族和 Windows 系列操作系统；另一方面是网络协议，常见的网络协议包括：TCP（Transmission Control Protocol，传输控制协议），IP（Internet Protocol，网络协议），UDP（User Datagram Protocol，用户数据报协议），SMTP（Simple Mail Transfer Protocol，简单邮件传输协议），POP（Post Office Protocol，邮局协议）和 FTP（File Transfer Protocol，文件传输协议），等等。

1.1.2　网络安全的层次体系

从层次体系上，可以将网络安全分成 4 个层次上的安全：物理安全，逻辑安全，操作系统安全和联网安全。

1. 物理安全

物理安全主要包括 5 个方面：防盗，防火，防静电，防雷击和防电磁泄漏。

（1）防盗：像其他物体一样，计算机也是偷窃者的目标，例如盗走软盘、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

（2）防火：计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎、吸烟、乱扔烟头等，使存在易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

（3）防静电：静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电放电火花，造成火灾。还可能使大规模集成电器损坏，这种损坏可能是不知不觉造成的。

（4）防雷击：利用引雷机理的传统避雷针防雷，不但增加雷击概率而且产生感应雷，而感应雷是电子信息设备被损坏的主要杀手，也是易燃易爆品被引燃起爆的主要原因。雷击防范的主要措施是，根据电气、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点作分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应做多层保护。

（5）防电磁泄漏：电子计算机和其他电子设备一样，工作时要产生电磁发射。电磁发射包括辐射发射和传导发射。这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，造成计算机的信息泄露。屏蔽是防电磁泄漏的有效措施，屏蔽主要有电屏蔽、磁屏蔽和电磁屏蔽 3 种类型。

2. 逻辑安全

计算机的逻辑安全需要用口令、文件许可等方法来实现。可以限制登录的次数或对试探操作加上时间限制；可以用软件保护存储在计算机文件中的信息；限制存取的另一种方式是通过硬件完成，在接收到存取要求后，先询问并校核口令，然后访问列于目录中的授权用户标志号。此外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如，多次登录或请求别人的文件。

3. 操作系统安全

操作系统是计算机中最基本、最重要的软件。同一计算机可以安装几种不同的操作系统。如果计算机系统可提供给许多人使用，操作系统必须能区分用户，以便防止相互干扰。

一些安全性较高、功能较强的操作系统可以为计算机的每一位用户分配账户。通常，一个用户一个账户。操作系统不允许一个用户修改由另一个账户产生的数据。

4. 联网安全

联网的安全性通过以下两方面的安全服务来达到。

（1）访问控制服务：用来保护计算机和联网资源不被非授权使用。

（2）通信安全服务：用来认证数据机要性与完整性，以及各通信的可信赖性。

1.2　研究网络安全的必要性

网络需要与外界联系，同时也就受到许多方面的威胁：物理威胁、系统漏洞造成的威胁、身份鉴别威胁、线缆连接威胁和有害程序威胁等。

1.2.1　物理威胁

物理威胁包括 4 个方面：偷窃、废物搜寻、间谍行为和身份识别错误。

1. 偷窃

网络安全中的偷窃包括偷窃设备、偷窃信息和偷窃服务等内容。如果想偷的信息在计算机里，一方面可以将整台计算机偷走，另一方面可以通过监视器读取计算机中的信息。

2. 废物搜寻

废物搜寻就是在废物（如一些打印出来的材料或废弃的软盘）中搜寻所需要的信息。在计算机上，废物搜寻可能包括从未抹掉有用东西的软盘或硬盘上获得有用资料。

3. 间谍行为

这是一种为了省钱或获取有价值的机密，采用不道德的手段获取信息的方式。

4. 身份识别错误

非法建立文件或记录，企图把它们作为有效的、正式生产的文件或记录，如对具有身份