计 算 机 系 列 教 材

网络安全技术教程

尹淑玲 主编

WUHAN UNIVERSITY PRESS
武汉大学出版社

计 算 机 系 列 教 材

网络安全技术教程

主 编 尹淑玲

副主编 蔡杰涛 魏 鉴 严 申 王传健

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

网络安全技术教程/尹淑玲主编. —武汉:武汉大学出版社,2014.5
计算机系列教材
ISBN 978-7-307-13113-2

Ⅰ.网… Ⅱ.尹… 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(2014)第 072165 号

责任编辑:辛 凯 责任校对:汪欣怡 版式设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)
(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)
印刷:湖北省京山德兴印务有限公司
开本:787×1092 1/16 印张:22.25 字数:562 千字
版次:2014 年 5 月第 1 版 2014 年 5 月第 1 次印刷
ISBN 978-7-307-13113-2 定价:45.00 元

前　言

在现今这样一个全球电子互联，电脑病毒和电子黑客充斥，电子窃听和电子欺诈肆虐的时代，安全已经不再是网络中一项可有可无的技术了，安全问题也无法再像过去一样可以一劳永逸地得以解决。网络安全技术与解决方案必须从根本上集成进网络的设备中，融入到网络的结构里。

网络安全技术教程的目标是理解网络安全理论以及所使用的工具和配置方法。本书内容丰富，包含了主流的安全产品、技术和解决方案。首先概括地介绍了网络安全和基本的网络威胁，然后依次介绍了网络设备安全、访问控制列表、局域网交换机安全、AAA 安全技术、防火墙技术、加密技术、VPN 技术、入侵检测和防御系统、网络操作系统安全、无线局域网安全和园区网络安全设计。针对每一部分网络安全理论，都结合主流安全产品，详细介绍了相应的配置方法，使读者通过对本书的学习，能够重点掌握和熟练运用相关的网络安全技术解决实际问题。

本书以 Cisco 公司的安全产品和技术为平台，在内容的选取、组织与编排上强调先进性、技术性和实用性，突出理论知识和实践操作的结合。在每章的最后，都配有习题供教师和学生课后复习使用，通过这些习题，读者可以进一步加深与巩固所学的知识。

本书可以作为本科类院校和高职高专类院校的相关专业的网络安全课程教材和参考书，也可以作为网络安全工程师、网络管理员以及广大网络爱好者的参考用书，还可以作为网络安全培训教材。

本书的前 9 章由武昌理工学院尹淑玲编写，第 10 章由王传健和严申编写，第 11 章由魏鉴编写，第 12 章由蔡杰涛编写，全书由尹淑玲统阅定稿。在本书的编写过程中，王化文教授给予了大力支持和鼓励，在此表示衷心的感谢。

由于网络安全涉及的技术领域较广，且作者水平有限，书中的不妥和错误在所难免，诚请各位专家、读者批评指正。编者也希望与读者多交流，联系方式为 yinslgirl@163.com。

编　者

2014 年 3 月

目 录

第1章 网络安全概述

随着网络技术及其应用的深入和普及，网络面临着越来越多的安全风险。潜在攻击者的数目随着网络规模的扩大而增长，而且这些攻击者可用工具的复杂度也在不断增加。网络安全是计算机网络中一个不可缺少的部分，它抵御内部和外部各种形式的威胁，以确保网络安全的过程。本章主要综述了网络安全的目标和策略，并提到了网络安全模型和评价标准。此外，还介绍了网络安全弱点和威胁，并详细阐述了几种可能威胁网络的攻击类型以及保护网络的安全组件和技术。

学习完本章，要达到如下目标：

◇ 理解网络安全的基本概念；
◇ 理解网络的弱点和安全威胁；
◇ 理解网络攻击的类型；
◇ 理解网络安全组件和技术。

1.1 网络安全简介

网络安全是一个系统。它不是防火墙，不是入侵检测，不是虚拟专用网，也不是认证、授权和统计(AAA)。网络安全也不是任何公司的安全产品和技术，尽管这些产品和技术在其中扮演了重要角色。那么对于网络安全来说什么是系统呢?

网络安全系统可以从广义上定义为：通过相互协作的方式为信息资产提供安全保障的全体网络设备、技术以及最佳做法的集合。

上述定义中的关键词是协作。实施基本路由器访问控制列表、状态化防火墙访问控制列表和基于主机的防火墙访问控制列表能实现许多基本的访问控制，但这些称不上是一个系统。对于一个真正的网络安全系统，必须是将可以协同运作的技术应用于一种特定的威胁模式。信息安全产业中的某些人将其称为“纵深防御”。例如，为了缓解 HTTP 蠕虫对公共 Web 服务器造成的威胁，我们可以采用如下系统元素，这些内容会在后面的章节中具体介绍。

◇ 对防火墙进行配置，使它可以防止一台遭到入侵的 Web 服务器继续感染不同网络中的其他系统。
◇ 网络入侵检测系统可以检测和阻止对 Web 服务器的感染企图。
◇ 主机入侵检测系统能够执行与网络入侵检测系统一样的功能，但它们比后者更接近主机，这也就意味着它们能够读取更多与特定攻击有关的内容数据。
◇ 更新特征数据库可以使防病毒软件具备检测特定蠕虫和其他恶意代码的功能。
◇ 及时打补丁、定期漏洞扫描、为操作系统设置密码锁定，以及实施 Web 服务器最佳做法等这些操作行为能够在防止系统威胁中起到重要作用。

上面所有系统元素的协同工作可以起到缓解威胁的作用。尽管其中的任何一项技术都无法100%有效地防止基于HTTP的蠕虫攻击，但针对特定威胁部署的协同技术越多，压制威胁的可能性也就越大。

1.1.1 网络安全目标

网络安全的目标是保护信息的机密性、完整性和可用性，这三个概念组成了CIA(Confidentiality Integrity Availability)三元组，它是最简单，适用范围也最广的安全模型。这三大核心原则既可以作为一切安全系统的指导方针，也可以作为衡量安全实施情况的准绳。

1. 机密性

机密性用于阻止未经授权就曝光敏感数据的行为。它可以确保网络达到了必要的机密级别，并且网络中的信息对非法用户是保密的。这些信息不仅指国家机密，而且也包括企业和社会团体的商业和工作机密，以及个人的机密信息，例如，在进行网上银行交易时，用户的银行账号信息。在CIA三元组中人们首先想到的一定就是确保网络的机密性，因此机密性也是最常遭受网络攻击的环节。密码学就是用来保护传输中的敏感数据，通过加密来确保在两台计算机间传输数据的机密性。

2. 完整性

完整性可以阻止未经授权就修改数据、系统和信息的行为，因此可以确保信息和系统的准确性。也就是说，如果数据是完整的，就等于这个数据没有被修改过，也就等于它和原始信息是一致的。有一种常见的攻击方式称为中间人(man-in-middle)攻击。在执行这类攻击时，攻击者就会在信息传递的过程中对其进行拦截和修改。

3. 可用性

可用性可以确保用户始终能够访问网络资源和信息，也就是说需要浏览这些信息时，这些信息总是能够访问的。确保授权用户可以随时访问信息非常重要。有一类攻击方式就是要设法让合法的用户无法正常访问数据，以达到中断服务的目的，拒绝服务(DoS)就是这类攻击方式之一。

尽管CIA三元组对安全目标的定义有其依据，但是以下两个概念也有必要加入安全领域。

- ◇ 可靠性：是指网络信息系统能够在规定条件下，在规定时间内，实现规定功能的特性。可靠性是网络安全最基本的要求之一，是所有网络信息系统建设和运行的目标。目前，对于网络可靠性的研究偏重于硬件方面，主要采用硬件冗余、提高可靠性和精确度等方法提高网络可靠性。实际上，软件的可靠性、人员的可靠性和环境的可靠性在保证系统可靠性方面也是非常重要的。
- ◇ 不可抵赖性：是指通信双方在通信过程中，对自己所发送或接收的消息不可抵赖，即发送者不能否认他发送过信息的事实和发送信息的内容，接收者也不能否认其接收到信息的事实和接收信息的内容。

1.1.2 网络安全策略

网络安全策略定义了一个框架，它基于风险评估分析以保护连接在网络上的资产，是一份全面的端到端文档。网络安全策略对访问连接在网络上的不同资产定义了访问限制和访问规则，是用户和管理员在建立、使用和审计网络时的信息来源，被用于辅助网络设计、传递

安全原则和促进网络部署。

就用户使用网络资源的易用性而言，有以下两种类型的安全策略。

◇ 许可性的策略：所有没有明确禁止的都是允许的。

◇ 限制性的策略：所有没有明确允许的都是禁止的。

通常，从安全的角度来说，有一个限制性的策略然后基于实际使用再对合法的使用展开通常是一个较好的想法。因为无论多么费力地试图堵住所有漏洞，许可性的策略还是会有漏洞存在的。

为了透彻理解什么是网络安全策略，需要对网络安全策略最重要的元素进行分析。RFC 2196 列出以下内容作为一个安全策略的要素。

◇ 计算机技术购买准则：指明了需要的或者涉及的安全特性。这些应该是对现有的购买策略和准则的补充。

◇ 保密策略：定义了如监控电子邮件、记录键盘输入和访问用户文件等与保密相关的合理的期望值。

◇ 访问策略：用于定义访问权利和特权，指定用户、工作团体和管理者可接受的使用准则，以便从失败或者泄密中保护资产。它应该提供指导原则，用以指导外部连接、数据通信、向网络中连接设备和向系统中添加新的软件。

◇ 职责策略：用于定义用户、工作团体和管理者的职责。它应该规定统计能力并且提供事故处理准则。

◇ 认证策略：通过一个有效的密码策略，为远程认证和认证设备使用设置准则，从而建立信任机制。

◇ 可用性声明：用于设置用户对资源可用性的期望值。它应该有地址冗余和恢复问题，也指明操作时间和维护停机时间。它还应该包括报告系统和网络故障的联系信息。

◇ 信息技术系统和网络维护策略：描述如何允许内部和外部维护人员处理和访问网络中用到的技术。

◇ 侵犯报告策略：用以指明哪种类型的侵犯(如保密和安全，内部的和外部的)是必须汇报的，以及报告生成后向谁汇报。

◇ 支持信息：它向用户、团队和管理者提供每种类型的策略侵犯的联系信息；如何处理关于一个安全事故的外部询问，或者什么应被考虑成保密或是专有的指导方针；以及安全程序的交叉引用和相关信息，如公司策略和政府的法律和法规。

定义了安全策略之后，下一步就是以网络安全设计的形式来实现这个策略。我们将要在本书中讨论不同的安全规则和设计问题。通常，网络安全设计中包含下列要素。

◇ 设备安全特性，如管理密码和不同网络组件中的 SSH；

◇ 防火墙；

◇ 远程访问 VPN 集中器；

◇ 入侵检测；

◇ 安全 AAA 服务器和其他网络上相关的 AAA 服务器；

◇ 不同网络设备上的访问控制和访问限制机制，如 ACL 和 CAR。

一旦实现了安全策略，继续对它分析、测试和改进是非常关键的。可以通过安全系统的正规化统计来实现这一点，也可以通过使用基于标准操作的度量方法日复一日地检测它来实现。

1.1.3 网络安全模型(PPDR)

PPDR(也被称为P2DR)是美国ISS公司提出的网络安全模型，它为网络安全解决方案提供思路和方法，它的组成包括策略(Policy)、防护(Protection)、检测(Detection)和响应(Response)，如图1-1所示。用户单位首先制定安全策略，指明安全防范的范围和目的，然后围绕策略采取合适的安全措施对目标实施安全防护，使用检测系统检查安全措施的有效性和网络系统活动的合法性，对违反安全策略的行为予以响应。

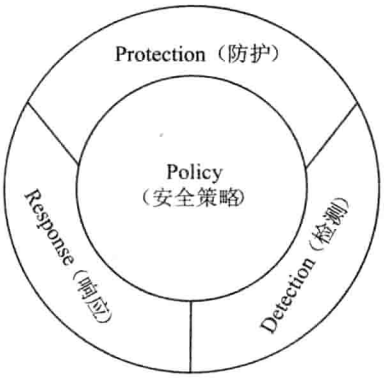

图1-1 PPDR安全模型

◇ 策略：安全策略是实现安全防护必须遵守的原则。安全策略是PPDR模型的核心，所有的防护、检测和响应都是依据安全策略实施的，企业安全策略为安全管理提供了管理方向和支持手段。

◇ 防护：是根据系统可能出现的安全问题而采取的预防措施，这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网(VPN)技术、防火墙、安全扫描和数据备份等。

◇ 检测：当攻击者穿透防护系统时，检测功能就发挥作用，与防护系统形成互补。检测是动态响应和加强防护的依据，也是强制落实安全策略的有力工具，通过不断的检测和监控网络及系统，来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。

◇ 响应：系统一旦检测到入侵，响应系统就开始工作，进行事件处理。响应包括紧急响应和恢复处理，恢复处理又包括系统恢复和信息恢复。

在PPDR模型中，安全策略是核心，防护、检测和响应是手段，它们组成了一个完整的、动态的安全循环体。PPDR认为安全具有动态性和整体性。动态性要求用户的防护技术和检测技术要适应策略的改变，不断更新进步；整体性要求安全策略的设计要着眼于整体系统的安全，而不能只抓系统局部安全。

1.1.4 网络安全评价标准

针对日益严峻的网络安全形势，许多国家和标准化组织纷纷出台了相关的安全标准，我国也制定了相应的安全标准，这些标准既有很多相同的部分，也有各自的特点。网络安全评

价标准中应用最为广泛的是1985年美国国防部制定的可信任计算机标准评价准则(Trusted Computer Standards Evaluation Criteria，TCSEC)。

1. 我国评价标准

我国于1999年10月经过国家质量技术监督局批准正式发布了《计算机信息系统安全保护等级划分准则》，其编号为GB17859-1999，该准则为安全产品的研制提供了技术支持，也为安全系统的建设和管理提供了技术指导。此准则将计算机安全保护划分为以下五个级别，从第一级到第五级，安全等级逐级增高，低级别安全要求是高级别安全要求的子集。

第一级为用户自主保护级(GB1安全级)：它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏。

第二级为系统审计保护级(GB2安全级)：除了具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有用户对自己行为的合法性负责。

第三级为安全标记保护级(GB3安全级)：除了继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。

第四级为结构化保护级(GB4安全级)：在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。

第五级为访问验证保护级(GB5安全级)：这一个级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

我国是国际标准化组织的成员国，信息安全标准化工作在各方面的努力下正在积极展开。从20世纪80年代中期开始，自主制定和采用了一批相应的信息安全标准。但是，标准的制定需要较为广泛的应用经验和较深入的研究背景，我国的信息安全标准化工作与国际已有的工作相比，还存在着这两个方面的差距，因此覆盖的范围还不够大，宏观和微观的指导作用也有待进一步提高。

2. 美国国防部评价标准

计算机网络系统的安全评价，通常采用美国国防部计算机安全中心制定的可信任计算机标准评价准则(TCSEC)，即网络安全橙皮书。自从1985年橙皮书成为美国国防部的标准以来，就没有改变过，多年来一直是评估多用户主机和小型操作系统的主要方法。其他子系统(如数据库和网络)也一直用橙皮书来解释评估。TCSEC定义了系统安全的五个要素：系统的安全策略、系统的审计机制、系统安全的可操作性、系统安全的生命期保证以及针对以上系统安全要素而建立和维护的相关文件。

TCSEC中根据计算机系统所采用的安全策略、系统所具备的安全功能将系统的安全级别从低到高分成四个级别：D类、C类、B类和A类，每类又分几个级别，如表1-1所示。

表1-1 **安全级别**

类别	级别	名称	主要特征
D	D	最低安全保护	没有安全保护
C	C1	自主安全保护	提供无条件的访问控制策略
	C2	有控制的访问保护	具有访问控制环境能力

续表

类别	级别	名称	主要特征
B	B1	标记的安全保护	强制存取控制，安全标记
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全域	存取控制、高抗渗透能力
A	A	验证设计	形式化的设计规范和验证技术

D 级(最小保护)是最低的安全级别，没有任何实际的安全措施，系统软件和硬件都容易被攻击。拥有这个级别的操作系统就像一个门户大开的房子，任何人都可以自由进出，是完全不可信任的。属于这个级别的操作系统有 DOS 和 Windows 98 等。

C1 级(自主安全保护)是 C 类的一个安全子级，它描述了一个典型的用在 UNIX 系统上的安全级别。这种级别的系统对硬件有某种程度的保护，如用户拥有注册账户和密码，系统通过账号和密码来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权，但硬件受到损害的可能性仍然存在。早期的 UNIX、NetWare V3.0 以下的操作系统均属于这个级别。

C2 级(有控制的访问保护)是 C 类中安全性较高的一级，除了包括 C1 级的安全策略与控制外，还增加了系统审计、访问保护和跟踪记录等特性。UNIX/Xenix 系统、NetWare V3.0 及以上系统和 Windows NT/2000 系统等均属于这个级别。

B1 级(标记的安全保护)是 B 类中安全性最低的一级，它是第一种需要大量访问控制支持的级别。B1 级除了满足 C 类要求外，还要求提供数据标记。系统必须对主要数据结构加载敏感度标签，还必须给出有关安全策略模型、数据标签和大量主体客体之间的出入控制的非形式陈述。系统必须具备精确标志输出信息的能力。

B2 级(结构安全保护)是 B 类中安全性居中的一级，它除了满足 B1 要求外，还要求计算机系统中所有设备都加标记，并给各设备分配单个或多个安全级别。

B3 级(安全域保护)是 B 类中安全性最高的一级，它使用安装硬件的方式来加强域的安全。例如，安装内存管理硬件来保护安全域免遭无授权访问或其他安全域对象的更改。该级别也要求用户通过一条可信任途径连接到系统上。

A 级(验证设计)是当前橙皮书的最高级别，它包含了一个严格的设计、控制和验证过程。该级别包含较低级别的所有安全特性。

1.2 网络安全弱点和威胁

网络的开放性和共享性在方便人们的同时，也使得网络系统容易受到攻击。目前，没有弱点和威胁的网络几乎是不存在的。在网络安全中，弱点可被归结为网络中存在的“软件漏洞”，而正是这些漏洞使得攻击能够成功。威胁是指对网络系统的网络服务、网络信息的机密性和可用性产生不利影响的各种因素，是一种可能会造成攻击的潜在危险。

1.2.1 弱点

在网络中弱点存在于网络和构成网络的每台设备中，每种网络和设备都有其固有的弱