信息安全理论与实践

Xinxi Anquan Lilun Yu Shijian

吴衡 董峰 著

国防工业出版社
National Defense Industry Press

信息安全理论与实践

吴衡　董峰　著

国防工业出版社
·北京·

内容简介

网络安全是计算机领域非常重要却又不容易掌握的内容之一。本书从最基本的网络协议开始讲起，直到网络安全领域软硬件的使用和配置操作，内容涉及网络安全扫描、入侵检测技术、防火墙技术和操作系统安全，以及各种理论的相关实践，如 Nmap 扫描软件、Snort 扫描软件、Iptables 防火墙软件等软件的安装、配置和使用。

本书内容翔实、结构清晰、循序渐进，并注意各个章节与实例之间的呼应和实践，既可以作为初学者的入门教材，也适用于有一定网络管理经验的技术人员学习和参考。

图书在版编目(CIP)数据

信息安全理论与实践/吴衡，董峰著. —北京：国防工业出版社，2015.2

ISBN 978-7-118-09913-3

Ⅰ.①信… Ⅱ.①吴… ②董… Ⅲ.①信息安全－安全技术 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2015)第 021646 号

※

國防工業出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本 710×1000 1/16 印张 12 字数 208 千字

2015 年 2 月第 1 版第 1 次印刷 印数 1—2500 册 定价 49.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

前　言

随着互联网的飞速发展，黑客、攻击和入侵等安全问题与日俱增，给网络的正常使用带来了很大的影响。考虑到网络数据的巨大价值，安全业务已持续成为各大公司和研究机构关注的重点。

为了应对这些挑战，国内外很多网络安全公司近年来相继开发出各种专用安全防范工具，如防火墙、入侵检测系统等，其价格动辄数万元甚至数十万元人民币。而各种宣传更是让用户眼花缭乱，众多的新概念、新产品让用户甚至技术人员无所适从。如何让技术人员更好地理解网络安全的核心理念，掌握与网络安全紧密相关的技术，就成为维护网络安全的前提条件。

本书从与网络安全有关的网络基础知识讲起，重点介绍网络扫描知识、防火墙技术、入侵检测技术和操作系统安全，为读者打开网络安全之门起到了抛砖引玉的作用。

本书既注重理论知识的讲解，更注重实际应用能力的培养与训练。主要内容如下：

第 1 章是基础理论。主要包括计算机的网络基础知识，重点介绍了网络协议和网络面临的主要威胁。本章是学习其他章节的基础知识，很多网络协议和概念在本章讲解，如 TCP/IP 协议、网络操作系统等。

第 2 章介绍网络扫描知识。无论是入侵网络还是攻击网络，网络扫描都是黑客的第一把尖刀，所以理解扫描的原理和实现手段对筑起网络安全第一道屏障起到相当大的作用。扫描有多种算法，如高速扫描、分布式扫描等。本章以 Nmap 为例，模拟真实网络环境，实验 Nmap 扫描器的用法。

第 3 章介绍防火墙知识。本章介绍不同类型的防火墙，及其工作原理和适用场合。防火墙的选择和配置是本章的重点，最后用 Iptables 实践练习了软件防火墙的搭建。

第 4 章介绍入侵检测技术。入侵检测是系统安全的一个重要环节，往往也是最后一环，对网络安全防范、网络犯罪取证具有重要的意义。本章从入侵检测的原理入手，分析不同入侵检测技术的优劣和各种入侵手段的检测方法。Snort 作为入侵检测的明星产品，本章分别针对两种主流操作系统的安装、配置和使用

进行了说明。

第5章介绍操作系统安全。本章讲解操作系统自身安全工作原理和操作系统的安全机制，以及针对操作系统的攻击和安全操作系统的设置。通过对Windows、Linux和Unix操作系统的安全机制配置的练习，加深读者对本章内容的掌握。

本书图文并茂、条理清晰、通俗易懂、内容丰富，操作步骤详细，方便读者上机实践；同时在难以理解和掌握的部分内容上给出相关提示，让读者能够快速地提高操作技能。

本书全文由吴衡同志编写，编写过程中参考了许多已出版发行的书籍、论文、著作以及互联网上公开的资料，从中得到了不少帮助和启发，由于篇幅有限，恕无法一一列出，在此对它们的作者表示衷心的感谢。

由于作者水平有限，本书不足之处在所难免，欢迎广大读者批评指正。

作 者

2014.10

目　录

第 1 章　计算机网络概述

1.1　计算机网络的基本概念

1.1.1　什么是计算机网络

计算机网络，是指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。通俗地讲，计算机网络是由多台计算机(或其他计算机网络设备)通过传输介质和软件物理(或逻辑)连接在一起组成的。

简单地说，计算机网络就是通过电缆、电话线或无线通信将两台以上的计算机互连起来的集合。

计算机网络的发展经历了面向终端的单级计算机网络、计算机网络对计算机网络和开放式标准化计算机网络三个阶段。

计算机网络由计算机、网络操作系统、传输介质(可以是有形的，也可以是无形的，如无线网络的传输介质就是看不见的电磁波)以及相应的应用软件四部分组成。

1.1.2　计算机网络的主要功能

计算机网络的主要功能是实现计算机之间的资源共享、网络通信和对计算机的集中管理，此外还有负载均衡、分布式处理和提高系统安全与可靠性等功能。

1. 资源共享

(1) 硬件资源：包括各种类型的计算机、大容量存储设备、计算机外部设备，如彩色打印机、静电绘图仪等。

(2) 软件资源：包括各种应用软件、工具软件、系统开发所用的支撑软件、语言处理程序、数据库管理系统等。

(3) 数据资源：包括数据库文件、数据库、办公文档资料、企业生产报表等。

(4) 信道资源：通信信道可以理解为电信号的传输介质。通信信道的共享是计算机网络中最重要的共享资源之一。

2. 网络通信

通信通道可以传输各种类型的信息，包括数据信息和图形、图像、声音、视频流等各种多媒体信息。

3. 分布处理

把要处理的任务分散到各个计算机上运行，而不是集中在一台大型计算机上。这样，不仅可以降低软件设计的复杂性，而且还可以大大提高工作效率和降低成本。

4. 集中管理

计算机在没有联网的条件下，每台计算机都是一个“信息孤岛”。在管理这些计算机时，必须分别管理。而计算机联网后，可以在某个中心位置实现对整个网络的管理，如数据库信息检索系统、交通运输部门的定票系统、军事指挥系统等。

5. 均衡负荷

当网络中某台计算机的任务负荷太重时，通过网络和应用程序的控制和管理，将作业分散到网络中的其他计算机中，由多台计算机共同完成。

1.1.3 计算机网络的特点

1. 可靠性

在一个网络系统中，当一台计算机出现故障时，可立即由系统中的另一台计算机来代替其完成所承担的任务。同样，当网络的一条链路出了故障时，可选择其他的通信链路进行连接。

2. 高效性

计算机网络系统摆脱了中心计算机控制结构数据传输的局限性，并且信息传递迅速，系统实时性强。网络系统中各相连的计算机能够相互传送数据信息，使相距很远的用户之间能够及时、快速、高效、直接地交换数据。

3. 独立性

网络系统中各相连的计算机是相对独立的，它们之间的关系是既互相联系，又相互独立。

4. 扩充性

在计算机网络系统中，人们能够很方便、灵活地接入新的计算机，从而达到扩充网络系统功能的目的。

5. 廉价性

计算机网络使计算机用户能够分享到大型机的功能特性，充分体现了网络系统的“群体”优势，能节省投资和降低成本。

6. 分布性

计算机网络能将分布在不同地理位置的计算机进行互连，可将大型、复杂的综合性问题实行分布式处理。

7. 易操作性

对计算机网络用户而言，掌握网络使用技术比掌握大型机使用技术简单，实用性也很强。

1.2 计算机网络的结构组成

一个完整的计算机网络系统是由网络硬件和网络软件所组成的。网络硬件是计算机网络系统的物理实现，网络软件是网络系统中的技术支持。两者相互作用，共同完成网络功能。

(1) 网络硬件：一般指网络的计算机、传输介质和网络连接设备等。

(2) 网络软件：一般指网络操作系统、网络通信协议等。

1.2.1 网络硬件的组成

计算机网络硬件系统是由计算机(主机、客户机、终端)、通信处理机(集线器、交换机、路由器)、通信线路(同轴电缆、双绞线、光纤)、信息变换设备(Modem，编码解码器)等构成。

1. 主计算机

在一般的局域网中，主机通常称为服务器，是为客户提供各种服务的计算机，因此对其有一定的技术指标要求，特别是主、辅存储容量及其处理速度要求较高。根据服务器在网络中所提供的服务不同，可将其划分为文件服务器、打印服务器、通信服务器、域名服务器、数据库服务器等。

2. 网络工作站

除服务器外，网络上的其余计算机主要是通过执行应用程序来完成工作任务的，这种计算机称为网络工作站或网络客户机。它是网络数据主要的发生场所和使用场所，用户主要是通过使用工作站利用网络资源并完成自己的作业。

3. 网络终端

网络终端是用户访问网络的界面，它可以通过主机联入网内，也可以通过通信控制处理机联入网内。

4. 通信处理机

通信处理机一方面作为资源子网的主机、终端连接的接口，将主机和终端连入网内；另一方面，它又作为通信子网中分组存储转发节点，完成分组的接收、校验、存储和转发等功能。

5. 通信线路

通信线路(链路)是为通信处理机与通信处理机、通信处理机与主机之间提供通信信道。

6. 信息变换设备

信息变换设备对信号进行变换，包括调制解调器、无线通信接收和发送器、用于光纤通信的编码解码器等。

1.2.2 网络软件的组成

在计算机网络系统中，除了各种网络硬件设备外，还必须具有网络软件。

1. 网络操作系统

网络操作系统是网络软件中最主要的软件，用于实现不同主机之间的用户通信，以及全网硬件和软件资源的共享，并向用户提供统一的、方便的网络接口，便于用户使用网络。目前网络操作系统有三大阵营，即 UNIX、NetWare 和 Windows。目前，我国最广泛使用的是 Windows 网络操作系统。

2. 网络协议软件

网络协议是网络通信的数据传输规范，网络协议软件是用于实现网络协议功能的软件。

目前，典型的网络协议软件有 TCP/IP 协议、IPX/SPX 协议、IEEE 802 系列标准协议等。其中，TCP/IP 是当前异种网络互连应用最为广泛的网络协议软件。

3. 网络管理软件

网络管理软件是用来对网络资源进行管理以及对网络进行维护的软件，如性能管理、配置管理、故障管理、计费管理、安全管理、网络运行状态监视与统计等。

4. 网络通信软件

网络通信软件是用于实现网络中各种设备之间进行通信的软件，使用户能够在不必详细了解通信控制规程的情况下，控制应用程序与多个站进行通信，并对大量的通信数据进行加工和管理。

5. 网络应用软件

网络应用软件是为网络用户提供服务，它研究的重点不是网络中各个独立

的计算机本身的功能，而是如何实现网络特有的功能。

1.2.3 计算机网络的拓扑结构

在组建计算机网络时，要考虑网络的布线方式，这也就涉及到了网络拓扑结构(Topology)的内容。网络拓扑结构是指网路中计算机线缆，以及其他组件的物理布局。

计算机网络常用的拓朴结构有总线型结构、环型结构、星型结构、树型结构。拓扑结构影响着整个网络的设计、功能、可靠性和通信费用等许多方面，是决定整个网络性能优劣的重要因素之一。

1. 总线型拓扑结构

总线型拓扑结构是指网络上的所有计算机都通过一条电缆相互连接起来，如图 1-1 所示。

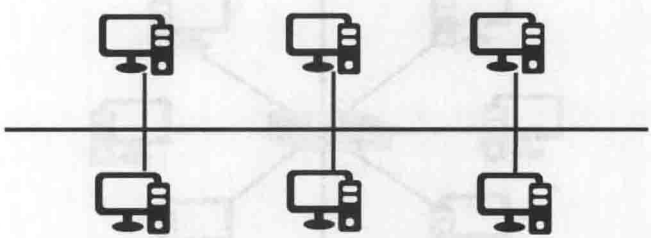

图 1-1 总线型拓扑结构示意图

在总线上，任何一台计算机在发送信息时，其他计算机必须等待。计算机发送的信息会沿着总线向两端扩散，从而使网络中所有计算机都会收到这个信息，但是否接收，还取决于信息的目标地址是否与网络主机地址相一致，即：若一致，则接受；若不一致，则不接收。连接在总线上的计算机必须相互协调，保证在任何时候只有一台计算机发送信号，否则会发生冲突。

在总线型网络中，信号会沿着网线发送到整个网络。当信号到达线缆的端点时，将产生反射信号，这种发射信号会与后续信号发送冲突，从而使通信中断。为了防止通信中断，必须在线缆的两端安装终结器，以吸收端点信号，防止信号反弹。

总线型网络不需要插入任何其他的连接设备。网络中任何一台计算机发送的信号都沿一条共同的总线传播，而且能被其他所有计算机接收。有时又称这种网络结构为点对点拓扑结构。

优点：它是最简单的一种拓扑结构，易于安装、成本费用低。

缺点：①传送数据的速度缓慢，共享一条电缆，只能有其中一台计算机发送信息，网络利用率低；②维护困难，因为网络一旦出现断点，整个网络将瘫痪，而且故障点很难查找。

2. 星型拓扑结构

每个节点都由一个单独的通信线路连接到中心节点上。中心节点控制全网的通信，任何两台计算机之间的通信都要通过中心节点来转接。因此中心节点是网络的瓶颈，这种拓扑结构又称为集中控制式网络结构，是目前使用最普遍的拓扑结构，处于中心的网络设备可以是集线器(Hub)也可以是交换机，如图 1-2 所示。

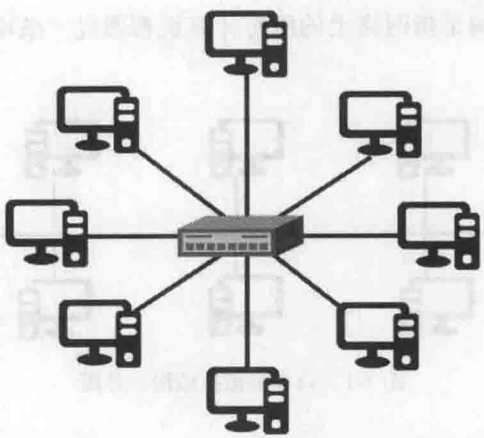

图 1-2　星型拓扑结构示意图

优点：结构简单、便于维护和管理，因为某台计算机或头条线缆出现问题时，不会影响其他计算机的正常通信，维护比较容易。

缺点：通信线路专用，电缆成本高；中心节点是全网络的可靠瓶颈，中心节点出现故障会导致网络的瘫痪。

3. 环型拓扑结构

环型拓扑结构，如图 1-3 所示，是以一个共享的环型信道连接所有设备，称为令牌环。在环型拓扑中，信号会沿着环型信道按一个方向传播，并通过每台计算机。而且，每台计算机会对信号进行放大后，传给下一台计算机。同时，在网络中有一种特殊的信号称为令牌。令牌按顺时针方向传输。当某台计算机要发送信息时，必须先捕获令牌，再发送信息。发送信息后在释放令牌。

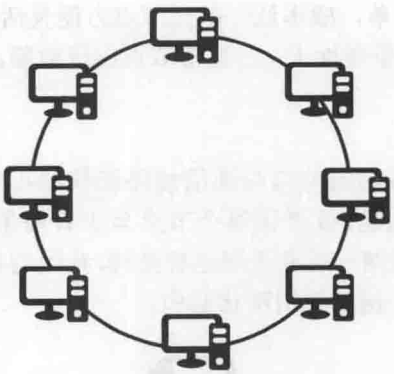

图 1-3　环型拓扑结构示意图

环型结构有两种类型，即单环结构和双环结构。令牌环(Token Ring)是单环结构的典型代表，光纤分布式数据接口(FDDI)是双环结构的典型代表。

环型结构的显著特点是每个节点用户都与两个相邻节点用户相连。

优点：①电缆长度短。环型拓扑网络所需的电缆长度和总线拓扑网络相似，但比星型拓扑结构要短得多。②增加或减少工作站时，仅需简单地连接。③可使用光纤，传输速度很高，适用于环型拓扑的单向传输。④传输信息的时间是固定的，从而便于实时控制。

缺点：①节点过多时，影响传输效率。②环的某处断开会导致整个系统的失效，节点的加入和撤出过程复杂。③检测故障困难。因为环型结构不是集中控制，故障检测需在网络各个节点进行，故障的检测就很不容易。

4. 树型拓扑结构

树型结构是星型结构的扩展，它由根节点和分支节点所构成，如图 1-4 所示。

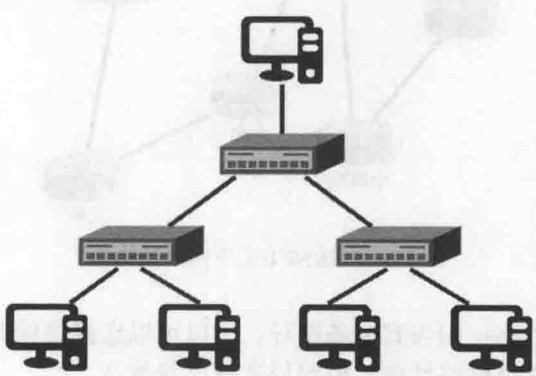

图 1-4　树型拓扑结构示意图