十三五 高等职业教育“十三五”精品规划教材（计算机网络技术系列）

网络安全技术项目化教程

主　编　段新华　宋风忠
副主编　伍又云　肖　玲

中国水利水电出版社
www.waterpub.com.cn

高等职业教育“十三五”精品规划教材

（计算机网络技术系列）

网络安全技术项目化教程

主　编　段新华　宋风忠

副主编　伍又云　肖　玲

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书基于项目化教学方式编写而成，体现“基于工作过程”与“教、学、做一体化”的教学理念。读者能够通过项目案例完成相关知识的学习和技能的训练，每个项目案例都具有典型性、实用性、趣味性和可操作性。

本书内容划分为9个项目共50个任务，具体包括：网络安全概述、网络安全技术基础、密码与加密技术、操作系统安全与加固、计算机病毒与木马、网络攻击与防范、防火墙、流量整形系统、日志管理系统。

本书可作为高等职业院校和高等专科院校“网络安全技术”课程的教学用书，也可作为成人高等院校、各类培训、计算机从业人员和爱好者的参考用书。

本书配有电子教案，读者可以从中国水利水电出版社网站和万水书苑免费下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com。

图书在版编目（CIP）数据

网络安全技术项目化教程 / 段新华，宋风忠主编
. -- 北京 : 中国水利水电出版社，2016.8
高等职业教育“十三五”精品规划教材. 计算机网络技术系列
ISBN 978-7-5170-4576-2

Ⅰ. ①网… Ⅱ. ①段… ②宋… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2016)第173844号

策划编辑：祝智敏　责任编辑：李　炎　加工编辑：李艳松　封面设计：李　佳

书　名	高等职业教育“十三五”精品规划教材（计算机网络技术系列） **网络安全技术项目化教程**
作　者	主　编　段新华　宋风忠 副主编　伍又云　肖　玲
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	北京泽宇印刷有限公司
规　格	184mm×260mm　16开本　16.5印张　407千字
版　次	2016年8月第1版　2016年8月第1次印刷
印　数	0001—3000册
定　价	39.00元

前　言

近年来，高等职业技术教育得到了飞速发展，急需适合职业教育特点的网络安全课程的实用型教材。我们编写的这本教材基于全国职业院校技能大赛网络信息安全项目，将项目内容分解为多个任务环节，通过任务来实现对相关知识点的理解和学习，减少了枯燥难懂的理论，增加了安全使用网络、安全管理网络等实际操作能力的培养与训练。

本书主要特点如下：

1．准确把握高职高专计算机网络专业人才的培养目标和特点，以项目为主线，以任务驱动及案例教学为核心。

2．教材以培养技术应用型人才为目标，以企业对人才的需要为依据，将技能培养和主流技术相结合，侧重培养学生的实战操作能力。通过项目实践，以案例为中心，围绕案例中所用到的知识点进行讲解，增强学生的职业能力，将书本中的知识转化为专业技能。

3．“教、学、做一体化”的编写模式。通过一个个教学任务或教学项目，在做中学，在学中做，边学边做，重点突出技能培养，同时介绍解决思路和方法，培养学生未来在就业岗位上的终身学习能力。

4．“易教易学”，教材所有案例都可以在虚拟机上完成，便于教师授课、学生预习和自主学习，免费提供教材的电子课件及工具软件等资源。

全书共有 9 个项目：

项目 1：网络安全概述

项目 2：网络安全技术基础

项目 3：密码与加密技术

项目 4：操作系统安全与加固

项目 5：计算机病毒与木马

项目 6：网络攻击与防范

项目 7：防火墙

项目 8：流量整形系统

项目 9：日志管理系统

本书可作为高职高专院校计算机网络技术专业和信息安全专业的教材，也可供从事网络安全管理的技术人员使用。

本书是教学名师、企业工程师和骨干教师共同策划编写的一本工学结合教材，由段新华和宋风忠担任主编，伍又云和肖玲担任副主编。中国水利水电出版社的有关负责同志对本书的出版给予了大力支持。在本书编写过程中参考了大量国内外计算机网络文献资料，在此，谨向这些著作者以及为本书出版付出辛勤劳动的同志表示感谢！

计算机网络安全技术发展迅速，书中不足之处在所难免，恳请广大读者提出宝贵意见。

作者 E-mail：sky99325@163.com。

编　者

2016 年 5 月

目　　录

1 网络安全概述

随着互联网的发展，人类享受着“随时、随地、随物”的三种维度的自由。越来越多的人更加离不开有网络的生活。网络安全不仅关系着国家的安全，更加关系着社会每个人的安全。

- 掌握网络安全的含义、网络安全威胁。
- 掌握安全体系的基本结构。

任务 1　网络安全引言

【任务描述】

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。信息这种重要的战略资源，也从原来的军事、科技、文化和商业渗透到当今社会的各个领域，它在社会生产、生活中的作用日益显著。通过网络，可将信息进行传播和共享，信息的传播是可控的，信息的共享是授权的，因此，信息的安全性和可靠性在任何状况下是必须要保证的。

【任务要求】

了解计算机网络安全涉及的应用。

【知识链接】

引言

计算机网络是信息社会的基础，已经进入社会的各个角落，经济、文化、军事和社会生活越来越多地依赖计算机网络。然而，开放性的网络在给人们带来巨大便利的同时，其安全性如何保证？因此，计算机网络的安全性成为信息化建设的一个核心问题。

计算机网络中存储、传输和处理的信息多种多样，许多是敏感信息，甚至是国家机密，例如政府宏观调控决策、商业经济信息、股票证券、科研数据等重要信息。由于网络安全漏洞，可能会造成信息泄露、信息窃取、数据篡改、数据破坏、计算机病毒、恶意发布等事件，由此造成的经济损失和社会危害难以估量。全世界计算机犯罪以每年大于100%的速度增长，网络的黑客攻击事件以每年10倍的速度增长。我国的计算机犯罪已经渗透到了许多方面，2011年12月，国内知名网站CSDN遭到黑客攻击，大量用户数据库被公布在互联网上，600多万个明文的注册邮箱被迫裸奔。在用户数据最为重要的电商领域，也不断传出存在漏洞、用户泄露的消息，据有关部门统计，我国90%以上的电子商务网站存在着严重的安全漏洞，网络安全面临着日益严重的威胁。

任务2　网络安全的含义

【任务描述】

什么是网络安全？每个接触计算机的人都会有这个疑问。理解网络安全的含义是学习和掌握它的基础。

【任务要求】

理解计算机网络安全的含义。

了解网络安全的特征。

【知识链接】

1. 什么是网络安全

全球信息化浪潮的影响日益加深，信息网络技术的应用日益普及，应用领域不断扩大，从传统的小型业务系统逐渐向大型的关键业务系统扩展，如党政机关的信息系统、企业商务系统、金融业务系统等，应用层次也在不断深入，伴随着网络的普及，安全成为影响网络化效能的重要因素。而互联网所具有的国际性、开放性和自由性在增加应用方便的同时，安全成了首要问题，是必不可忽视的重要组成部分。

网络安全在不同的应用场合和不同的应用对象中，称呼不一，因此网络安全有许多不同的说法。网络安全又被称为网络信息安全、信息网络安全、信息安全、网络安全威胁、网络安全攻防和网络安全技术等，在不引起错误的情况下，为描述问题方便，在不同的章节可能会引用其中一种说法。网络安全包括解决或缓解计算机网络技术应用过程中存在的安全威胁的技术

手段或管理手段，也包括这些安全威胁本身及相关的活动。网络安全的不同说法代表网络安全不同角度和不同层面的含义，网络安全威胁和网络安全技术是网络安全的最基本的表现。

网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的机密性、完整性及可使用性受到保护。根据网络安全的特点，网络安全问题包括两方面的内容：一是网络本身的系统安全，二是网络的信息安全。而网络安全的最终目的是信息安全，要想信息安全必须保证网络系统软件、应用软件、数据库系统具有一定的安全保护功能，并保证网络部件，如终端、调制解调器、数据链路的功能仅仅能被那些被授权的人访问。

从广义上来说，凡是涉及网络上信息的保密性、完整性、可用性、不可否认性和可控制性的相关技术和理论都是网络安全的领域。保密性是指信息不暴露给未授权的实体或进程；完整性是指只有得到授权的实体才能修改数据，并且能够判别出数据是否已被篡改；可用性说明得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作；可控性表示可以控制授权范围内的信息流向及行为方式；可审查性指对出现的网络安全问题提供调查的依据和手段。

网络安全的具体含义随观察者角度不同而不同。对安全保密部门来说，希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免给国家造成损失，避免对社会产生危害。从社会教育和意识形态来说，网络上不健康的内容会对社会的稳定和人类的发展造成威胁，会影响青少年的发展，必须对其进行控制。从网络运行和管理者角度来说，希望其网络的访问、读写等操作受到保护和控制，避免出现后门、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御黑客的攻击。从用户个人、企业等的角度来说，希望涉及个人隐私或商业利益的信息在网络上传输受到机密性、完整性和不可否认性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯，也就是说用户的利益和隐私不被非法窃取和破坏。

2. 网络安全的特征

网络的安全，就是要保障网络的信息安全。信息安全的特征有哪些呢？

（1）保密性。

保密性是指信息不暴露给未授权的实体或进程。

（2）完整性。

完整性是指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、破坏和丢失的特性。

（3）可用性。

可用性指网络信息可被授权实体正确访问，并按要求能正常使用，或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息。当系统遭受攻击或破坏时，能迅速恢复并能投入使用。比如网络环境下的拒绝服务，破坏网络和有关系统的正常运行等都属于对可用性的攻击。

（4）不可否认性。

不可否认性是指通信双方在信息交互过程中，确信参与者本身以及参与者所提供的信息的真实同一，即所有参与者都不可否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

（5）可控性。

可控性指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定的传输范围和存放空间内可控，除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

任务 3　网络安全体系结构

【任务描述】

了解网络的体系结构，不同层有不同的安全隐患，针对这些隐患可以更充分地预警。网络安全体系结构详细地说明了网络的划分。

【任务要求】

了解计算机网络安全的体系结构。

【知识链接】

1. OSI 参考模型

将不同地理位置的具有独立功能的多台计算机系统，通过通信设备和线路互相连接起来，就组成了计算机网络。计算机网络可以看成多台计算机的集合，每台计算机独立自治，具有完整的计算机系统，每台计算机之间又相互联系，可以交换信息数据，通过网络可以实现资源共享等功能，为人们的生活提供了很大的方便。

计算机之间的连接由硬件实现，可以有不同的介质，无线电、激光、卫星微波等。计算机之间的信息交换分为物理和逻辑两种形式，物理含义指的是通过比特流传输实现直接相连的两台计算机之间的信息交换，逻辑含义是指计算机之间交换的信息具有一定的逻辑结构，直接或间接地代表用户需要的形式。简单来说，物理交换通过硬件来实现，逻辑交换通过软件来实现。

计算机之间进行的通信传输，必须遵守相应的通信规则，使用同样的通信协议。计算机网络通信协议通过程序来实现，大多数网络采用了分层的体系结构，每一层实现不同的功能。

1985 年，国际标准化组织（International Standard Organization）提出了一种网络互连模型 OSI（Open System Interconnect）。OSI 是一种开放式互连的体系结构，一般又称 OSI 模型，这种模型将网络体系结构划分为七层，由上到下分别为应用层、表示层、传输层、会话层、网络层、数据链路层、物理层。OSI 模型及所对应的功能如表 1-1 所示。

表 1-1　OSI 模型的各层功能图

OSI 模型	主要功能
应用层	网络服务与用户应用程序间的一个接口
表示层	数据传递的语法与语义（数据表示、数据安全、数据压缩）
传输层	会话的建立、管理和终止

续表

OSI 模型	主要功能
会话层	用一个寻址机制来标识一个端口号
网络层	基于网络层地址（IP 地址）进行不同网络系统间的路由选择
数据链路层	物理链路上无差错地传送数据帧(通过使用接收系统的硬件地址或物理地址来寻址)
物理层	建立、维护和取消物理连接

发送进程传输给接收进程的数据，通过物理层逐层传输到应用层，接收进程的数据传输正好是反过程。

2. TCP/IP 协议

OSI 参考模型只是描述了一些概念，用来协调进程间通信标准的制定，并没有提供一个可以实现的方法。在现实网络世界里，应用更多的是 TCP/IP(Transmission Control Protocol/Internet Protocol，传输控制协议/网际互联协议)。TCP/IP 也是一个开放模型，与 OSI 参考模型相比，其结构更加简单，TCP/IP 是因特网最基本的协议，也是因特网的基础，它是由多个协议组成的协议组，是互联网使用的标准协议。目前，几乎每个重要的操作系统都支持 TCP/IP 进行网络传播。

与 OSI/RM 不同，TCP/IP 体系分为四个功能层，从上到下依次是应用层、传输层、网络层、网络接口层。和 OSI 参考模型对应关系如表 1-2 所示。

表 1-2 TCP/IP 体系与 OSI 参考模型对应关系表

TCP/IP 体系	OSI 参考模型
应用层	应用层
	表示层
	会话层
传输层	传输层
网络层	网络层
网络接口层	数据链路层
	物理层

TCP/IP 体系结构各层功能如下：

（1）应用层。

应用层是体系结构的最高层，直接为用户的进程服务，应用层可提供不同需求和特性的管理服务和应用服务。常见的有万维网应用(HTTP 协议)、远程登录(Telnet)、电子邮件(SMTP 协议、POPs)、文件传输（FTP 协议)、网络管理（SNMP)、域名系统（DNS）等。

（2）传输层。

传输层的功能是向两个主机中的进程之间提供通信服务。传输层为信源节点和目的节点间的通信提供端到端的数据传输，而通信子网只能提供邻节点之间点到点的传输。由于传输层为多个进程提供通信服务，为了区别，传输层使用端口区分进程。传输层的协议主要有 TCP 和 UDP。

TCP 协议，即传输控制协议，是一种面向连接的服务，可以提供可靠的数据传输。

UDP 协议，即用户数据报协议，是一种无连接的协议，不能提供可靠的数据传输。

（3）网络层。

网络层通常又称为 IP 层，提供两个主机之间的通信服务。其主要功能是分组转发和路由选择，实现网络中点对点互连。网络层通过 IP 地址区分不同的主机，主机和通信设备通过 IP 地址选择合适的路由。

（4）网络接口层。

网络接口层又称为数据链路层，实现了网络中相邻设备之间的互连。在相邻的两个节点之间传输数据时，数据链路层将 IP 层传下来的数据封装成帧，然后通过物理层传送到路由器或目的主机，在共享传输介质的网络中，链路层通过 MAC 地址区分目的主机。

3. 安全体系

计算机网络系统的安全体系综合多方面进行考虑，如图 1-1 所示。

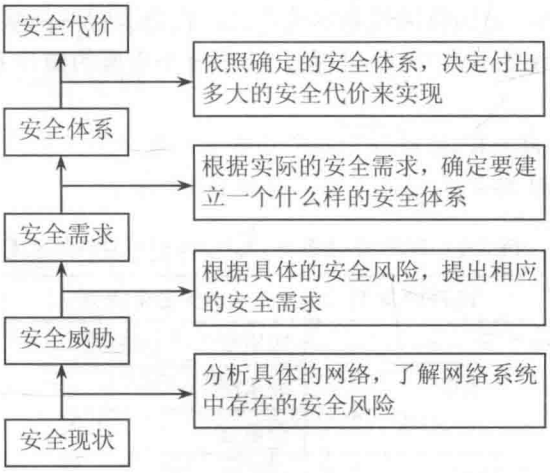

图 1-1　计算机网络系统的安全体系

任务 4　网络安全威胁

【任务描述】

人们利用通信网络将独立的计算机连接起来，随之而来产生的安全问题也是人们必须要研究解决的。那么，有哪些因素对网络的安全构成威胁呢？

【任务要求】

了解网络安全的威胁原因。

了解网络安全的威胁现状。

了解网络安全的威胁发展趋势。

【知识链接】

1. 网络系统自身的脆弱性

网络安全不仅包括信息安全，还有系统自身的安全，二者缺一不可。信息安全主要是各种信息的存储、传输的安全，主要体现在保密性、完整性、可控性和不可否认性上；系统安全主要有网络设备的硬件、操作系统和应用软件的安全。对于系统安全威胁，主要是由于计算机网络系统自身的原因，可能存在不同程度的脆弱性，为各种动机的攻击提供了入侵、骚扰和破坏系统的途径和方法。

（1）硬件系统。

网络硬件系统的安全隐患主要表现在物理安全方面的问题。计算机或网络设备，包括主机、显示器、电源、交换机、路由器等，除了难以抗拒的自然灾害外，温度、湿度、静电、电磁场等也可能造成信息的泄露或失效，甚至危害使用者的健康和生命安全。

（2）软件系统。

软件系统的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞，如“冲击波”病毒就是针对操作系统中的漏洞实施攻击。软件系统的安全隐患主要表现在操作系统、数据库和应用软件上。

（3）网络和通信协议。

Internet 上普遍使用的标准主要基于 TCP/IP 架构。TCP/IP 在设计上存在着一定不足，对于安全问题，不能提供通信所需的安全性和保密性。虽然 TCP/IP 经历了多次改版升级，但由于协议本身的原因，未能彻底解决自身的安全问题，存在以下隐患。

①缺乏用户身份鉴别机制。TCP/IP 使用 IP 地址作为网络节点的唯一标识，而 IP 地址很容易被伪造或更改。TCP/IP 没有树立对 IP 包中源地址真实性的鉴别和保密机制，因此，Internet 上任何一台主机都可以假冒另一台主机进行地址欺骗，使得网上传输数据的真实性无法得到保证。

②缺乏路由协议鉴别机制。TCP/IP 在 IP 层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别和保护。因此，可以通过 Internet 利用路由信息修改网络传输路径，误导网络分组传输。

③缺乏保密性。TCP/IP 数据流采用的明文传输方式无法保障信息的保密性和完整性。

④TCP/UDP 的缺陷。TCP/UDP 是基于 IP 上的传输协议，TCP 分段和 UDP 数据包是封装在 IP 包中传输的，除可能面临 IP 层所遇到的安全威胁外，还存在 TCP/UDP 实现中的安全隐患。例如，攻击者可以利用 TCP 建立所需要的“三次握手”，使 TCP 连接处于“半打开状态”，实现拒绝服务攻击。UDP 是个无连接协议，极易受到 IP 源路由和拒绝服务攻击。

⑤TCP/IP 服务的脆弱性。各种应用层服务协议（如 FTP、DNS、HTTP、SMTP 等）本身存在安全隐患，涉及身份鉴别、访问控制、完整性和机密性多个方面。

2. 网络安全威胁现状

随着网络应用在越来越多的领域，大量数据信息存储在计算机上，如政府机关大量的机密文件，军事研究的重要数据，企业的商业秘密，个人的账号信息等。这些信息的安全受到很多威胁甚至是攻击，一些非法入侵他人网络的人，窃取和篡改机密材料和个人信息，破坏网络通信等。据专家分析，我国大部分的网站是不安全的，有些网站可以轻易被入侵，给人们的生活带来不愉快和尴尬的事例屡见不鲜。

网络安全威胁是指实体对网络资源的保密性、完整性和可用性在合法使用时可能造成的危害，这些可能出现的危害，是受某些别有用心的人通过一定的攻击手段来实现的。网络系统的安全威胁主要表现在主机可能会收到非法入侵者的攻击，网络中的敏感数据可能会泄露或被修改，从内部网向公众网传送的信息可能被他人窃听或篡改等。

网络安全威胁根据攻击方式不同，可划分为主动攻击方式和被动攻击方式两大类，主要有以下几个方面。

- 截获：攻击者从网络上窃听他人的通信内容；
- 中断：攻击者有意中断他人在网络上的通信；
- 篡改：攻击者故意篡改网络上传送的通信内容；
- 伪造：攻击者伪造网络上的通信内容并进行传送。

上述攻击方式中，截获信息属于被动攻击，中断、篡改和伪造是主动攻击。除此之外，网络威胁还有许多攻击方式，例如计算机病毒、计算机蠕虫、特洛伊木马和逻辑炸弹等多种恶意程序。近年来，计算机病毒都是与网络结合，同时具有多种攻击手段和传播方式，病毒技术与黑客技术的结合对信息安全会造成更大的威胁，潜在的威胁和损失将会更大。安全威胁与互联网相结合，利用一切可利用的资源，如电子邮件、远程管理即时通信工具等方式进行传播。从发展趋势来看，现在的病毒已经由相对单一传播的单种行为，逐渐发展成多种传播的复杂方式，集黑客、木马于一体的电子邮件、文件传染等方式对用户的利益造成很大的威胁，新的网络安全威胁破坏性极强，欺骗性强，利用系统的安全漏洞，扩展速度极快。随着手机、平板等无线终端设备的普及，出现了很多对于无线网络的安全威胁，使用远程网络攻击，手机流量无故增大，用户密码泄露，手机被窃听等，很多用户的隐私被泄露。

3. 网络安全威胁的原因

根据网络安全威胁的各种方式，原因有以下几点：

（1）系统的开放性。

共享、开放是计算机网络的优势和目的，但随着开放系统应用环境的不同，开放对象的多种多样以及开放规模的增大，网络安全威胁存在隐患。

（2）系统的复杂性。

随着计算机硬件规模及软件规模的不断增大，设计环境和应用环境的差异，使得设计不可能“完美无瑕”，不可避免地将会导致软件漏洞、硬件漏洞、设计缺陷等问题。复杂的系统使得安全威胁的可能性更大，设计人员才会投入大量的人力、物力、财力来不断完善设计系统，减小安全威胁的风险。

（3）人为因素。

网络系统的最终使用者是人，人与人之间的差异不可避免地会造成网络安全威胁。现实社会还会存在违法犯罪，网络的世界也不例外，计算机犯罪的事例屡见不鲜，人为因素是网络安全威胁的最大隐患。

4. 网络安全威胁趋势

随着互联网规模扩大和用户的级数增加，网络安全攻击和威胁的形式将更加严峻。网络安全威胁的新趋势如下：

（1）攻击行为政治化。

电子政务的建设和其他安全需求部门的网络系统的普及，网络攻击行为不仅仅是简单的

恶意行为，更涉及到国家的安危、机密。以政治破坏为目的的危害国家利益的网络攻击行为在不断升级，更成为网络安全威胁发展的新趋势。

（2）攻击行为智能化。

随着计算机技术的进步，越来越多的攻击技术已被封装成一些免费的工具，在用户不经意的时候自动利用工具，网络攻击的自动化以及攻击速度越来越高。

（3）攻击行为的不对称性。

互联网上的安全是相互依赖的，全球每个互联网系统的安全状态都会影响其相连的网络系统遭受攻击的可能性，由于计算机分布式技术的不断发展，攻击者可以利用分布式系统，轻易地对受害者发动攻击，破坏系统的安全，分布式技术使得网络安全的威胁增大。

（4）对基础设施的攻击。

基础设施攻击是大面积影响互联网组成部分的攻击。由于用户越来越多地依赖互联网完成日常事务，因此攻击基础设施会严重影响人们的日常生活，造成大面积瘫痪。基础设施的攻击行为主要有分布式拒绝服务攻击、蠕虫病毒、对互联网域名系统的攻击、对路由器攻击和利用路由器的攻击。

（5）病毒与网络攻击融合。

互联网普及程度不高时，病毒行为和网络攻击行为界限分明，而现阶段病毒行为和网络攻击之间是相互联系着的，很难有分明的界限，网络成为病毒传播的主要途径，病毒技术、黑客技术与互联网结合可以形成更严重的攻击效果。

【思考与练习】

理论题

1. 网络安全的含义是什么？
2. 简述网络面临的安全威胁。

2

网络安全技术基础

同现实生活一样，网络攻击者在开始入侵之前，往往要对对方的计算机进行一系列的“踩点”活动，将最大限度地获得对方的信息，然后从这些信息中找到对方的计算机漏洞，进行完准备工作再一举入侵，成功攻击对方计算机。

- 掌握常用的网络安全命令。

任务 1　网络基础介绍

【任务描述】

错综复杂的网络和数百上千的计算机怎么才能正常连接？主机之间相互不干涉能正常运作，数据又是如何正确地通过网络上传和下载的呢？计算机能通过网络共享资源，那么网络的安全就成为首要考虑的问题，也就是如何能保证系统连续可靠正常地运行，网络服务不中断。通过了解网络技术的一些基本知识能更好地理解网络是如何运行的。

【任务要求】

了解关于网络 IP 地址及端口的一些相关知识。

【知识链接】

1. IP 地址

Internet 网络上连接着数千百万的计算机主机，人们给每台主机都分配了一个联网专用的逻辑地址以区别这些主机，这个专门的地址称为 IP 地址。IP 地址具有唯一性，不重复，因此通过 IP 地址就可以访问世界上的任意一台计算机主机。

IP 地址由 4 部分十进制数字组成，各部分之间用小数点隔开，每部分十进制数字对应一个 8 位二进制数，共 32 位二进制数，例如，某台计算机主机的 IP 地址为 106.42.133.238。地址空间的不足必将妨碍互联网的进一步发展。为了扩大地址空间，拟通过 IPv6 重新定义地址空间，IPv6 采用 128 位地址长度。

IP 地址现由因特网名字与号码指派公司 ICANN（Internet Corporation for Assigned Names and Numbers）分配，Internet 的 IP 地址由 NIC（Internet Network Information Center，因特网信息中心）统一负责全球地址的规划、管理。同时由 Inter NIC 具体负责美国及其他地区的 IP 地址分配；APNIC （Asia Pacific Network Information Center）负责亚洲地区的 IP 地址分配；ENIC 负责欧洲及其他地区的 IP 地址分配。

- 固定 IP：固定 IP 地址是长期固定分配给一台计算机使用的 IP 地址，一般只有特殊的服务器才拥有固定 IP 地址。
- 动态 IP：由于 IP 地址资源非常短缺，电话拨号上网或者普通宽带上网用户一般不具备固定 IP 地址，而是由 ISP 动态分配暂时的一个 IP 地址。用户一般不需要去了解动态 IP 地址，这些是由计算机系统自动完成的。
- 公有地址（Public Address）：由 Inter NIC 负责。这些 IP 地址分配给注册并向 Inter NIC 提出申请的组织结构，通过它可以直接访问因特网。
- 私有地址（Private Address）：属于非注册地址，专门为组织结构内部使用，以下列出留用的内部私有地址：

  A 类：10.0.0.0～10.255.255.255

  B 类：172.16.0.0～172.31.255.255

  C 类：192.168.0.0～192.168.255.255

2. 计算机端口

（1）什么是端口。

端口（Port）可以认为是设备与外界通信交流的出口。端口的含义有以下两种：

物理端口：又称为接口，是可见端口，主要用于连接其他网络设备。如交换机、路由器、集线器等的 RJ-45 端口，计算机背板的 RJ-45 网口，MODEM的 Serial 端口，电话使用的 RJ-11 插口等。

逻辑端口：一般是指 TCP/IP 中的计算机或交换机、路由器内的端口，不可见。端口号的范围为 0～65535，如用于 FTP 服务的 21 端口；用于浏览网页服务的 80 端口等。

在 Internet 上，各主机间通过 TCP/IP 协议发送和接收数据包，各个数据包根据其目的主机的 IP 地址来进行互联网络中的路由选择，把数据包顺利地传送到目的主机。大多数操作系统都支持多程序（进程）同时运行，那么目的主机应该把接收到的数据包传送给众多同时运行

的进程中的哪一个呢？为了解决这个问题，引入了端口机制。

本地操作系统会给那些有需求的进程分配协议端口（protocol port），每个协议端口由一个正整数标识，如 80、139、445 等。当目的主机接收到数据包后，将根据报文首部的目的端口号，把数据发送到相应端口，而与此端口相对应的那个进程将会领取数据并等待下一组数据的到来。

端口其实就是队，操作系统为各个进程分配了不同的队，数据包按照目的端口被推入相应的队中，等待进程取用，在极特殊的情况下，这个队也是有可能溢出的，不过操作系统允许各进程指定和调整自己队的大小。不光接收数据包的进程需要开启它自己的端口，发送数据包的进程也需要开启端口，这样，数据包中将会标识有源端口，以便接收方能顺利地回传数据包到这个端口。

（2）详解端口。

如果把 IP 地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口最多可以有 65536 个。端口是通过端口号来标记的，端口号只有整数，范围是 0～65535。不同的服务如 Web 服务、FTP 服务、SMTP 服务等通过不同的端口门进入到拥有 IP 地址的主机这个大房子中来实现。由上可以看出，一个 IP 地址可以对应多个网络服务，显然主机不能只靠 IP 地址来区分不同的网络服务，实际上通过“IP 地址+端口号”来区分不同的服务。换言之，如果没有端口，每一个服务进程要占用一个 IP 地址，这是一种极大的浪费。

一般一个端口对应一个应用程序，发送到这个端口的数据被这个应用程序接收，但是一个应用程序可以对应多个端口。

（3）端口类型。

- 公认端口（Well Known Ports）：范围是 0～1023，一般固定分配于一些服务。例如 80 端口分配给 WWW 服务，21 端口分配给 FTP 服务等。
- 注册端口（Registered Ports）：范围是 1024～49151，分配给用户进程或应用程序。这些进程主要是用户选择安装的一些应用程序，而不是已经分配好了公认端口的常用程序。这些端口在没有被服务器资源占用的时候，可以由用户端动态选用为源端口。例如，许多系统处理动态端口从 1024 左右开始。
- 动态端口（Dynamic Ports）：范围是 49152～65535。之所以称为动态端口，是因为它一般不固定分配某种服务，而是动态分配。

3. 端口扫描及端口扫描器

端口扫描是指某些别有用心的人发送一组端口扫描消息，试图以此侵入某台计算机，并了解其提供的计算机网络服务类型（这些网络服务均与端口号相关）。攻击者可以通过它了解到从哪里可探寻到攻击弱点。实质上，端口扫描包括向每个端口发送消息，一次只发送一个消息。接收到的回应类型表示是否在使用该端口并且可由此探寻弱点。

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以不留痕迹地发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本，这样就能间接或直观地了解到远程主机所存在的安全问题。