浙江省“十一五”高校重点教材

全国高职高专计算机立体化系列规划教材

计算机系统安全与维护

主　编　吕新荣　陆世伟

所有实践操作都可以在虚拟机搭建的网络上完成

每个项目都由典型的工作任务构成

北京大学出版社
PEKING UNIVERSITY PRESS

全国高职高专计算机立体化系列规划教材
浙江省“十一五”高校重点教材

计算机系统安全与维护

主　编　吕新荣　陆世伟
副主编　侯小丽　陈致远
　　朱　珍

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

本书紧密结合当前国际和国内计算机信息安全的发展趋势，用通俗易懂的语言概括介绍了计算机信息安全理论基础知识，包括信息安全的概念和基本原理、相关道德和法律知识、各种网络攻击和威胁、防火墙、入侵检测系统、Windows 系统管理、Windows 域管理、数据加密、网络安全通信等。本书按照项目课程设计理念，将来源于企业的实际案例设计成教学项目，以业界知名的网络安全产品为载体，使读者在完成项目的过程中掌握计算机信息安全基础知识和基本技能。本书每章后均附有思考练习，能够帮助读者拓展提高，对计算机信息安全技术和产品有更深入和广泛的理解。

本书适合作为高职高专计算机类和信息安全类专业及相近专业的教材，也可作为中小企业信息系统管理员、网络管理员、信息安全员的培训教材或工作参考书。

图书在版编目(CIP)数据

计算机系统安全与维护/吕新荣，陆世伟主编. —北京：北京大学出版社，2013.1

(全国高职高专计算机立体化系列规划教材)

ISBN 978-7-301-21754-2

Ⅰ. ①计… Ⅱ. ①吕…②陆… Ⅲ. ①计算机系统—安全技术—高等职业教育—教材②计算机系统—维修—高等职业教育—教材 Ⅳ. ①TP30

中国版本图书馆 CIP 数据核字(2012)第 294581 号

书　　名：计算机系统安全与维护

著作责任者：吕新荣　陆世伟　主编

策 划 编 辑：李彦红　刘国明

责 任 编 辑：刘国明

标 准 书 号：ISBN 978-7-301-21754-2/TP・1263

出 版 发 行：北京大学出版社

地　　址：北京市海淀区成府路 205 号　100871

网　　址：http://www.pup.cn　　新浪官方微博：@北京大学出版社

电 子 信 箱：pup_6@163.com

电　　话：邮购部 62752015　发行部 62750672　编辑部 62750667　出版部 62754962

印　刷　者：北京世知印务有限公司

经　销　者：新华书店

787 毫米×1092 毫米　16 开本　15.75 印张　363 千字

2013 年 1 月第 1 版　　2013 年 1 月第 1 次印刷

定　　价：30.00 元

前　言

随着我国经济的高速发展和信息化建设的不断深入，越来越多的中小企业都已经完成了企业网络的建设，很多企业开始利用信息技术手段来改善企业流程，提高市场竞争力，越来越多的企业也意识到信息是企业的重要财富和竞争法宝。信息背后潜在的巨额利润也勾起了某些人的欲望，“泄密”、“盗号”等事件屡见报端，各种“门事件”的发生也表明信息安全事件随时有可能发生在普通人的身上。普及信息安全教育和培养掌握信息安全知识和技能的人才已经成为信息时代非常迫切的一项任务。

从调查统计结果来看，我国绝大多数中小企业没有专门的信息安全管理人员，企业的信息安全管理一般由网络管理人员承担。不同于专业网络安全公司的技术研发人才，中小企业的网络管理人员需要能利用成熟的网络安全设备、技术和手段保障企业的网络安全运行。这种岗位特点给相关课程教学带来了较大挑战，网络安全设备大都比较昂贵，如果依据设备进行教学则投入成本较大，但如果以讲解信息安全理论知识为主则比较抽象枯燥，学生不愿意学。本书根据编者多年的教学讲义重新编写，在编写过程中着重体现以下特色。

(1) 采用“项目—任务”方式编写，每个项目都由典型的工作任务构成，在完成任务的过程中掌握信息安全相关知识和技能；

(2) 利用软件代替硬件设备，比如防火墙和 VPN 采用 ISA Server 2006、入侵检测系统采用 Snort 等，既可以让学生掌握各种技术的原理，又避免了大量的硬件投入；

(3) 本书的所有实践操作都可以在虚拟机搭建的网络上完成。“云计算”是 IT 产业的未来趋势，而虚拟化技术是“云计算”的基石，利用虚拟机构建网络既可以培养学生网络构建的技能，又可以为学生从事将来的“云计算”相关工作打下基础；

(4) 注重培养信息安全素养和学习能力。信息安全不仅需要从业者具有良好的技能，更需要具有良好的职业素养和道德法律意识。同时信息安全是一个快速发展的领域，需要从业者具有良好的学习能力。

本书分为 8 个项目：项目 1 计算机网络安全认识、项目 2 网络病毒防范、项目 3 网络攻击防范、项目 4 网络安全加固、项目 5 Windows 安全管理、项目 6 数据安全管理、项目 7 Windows 域安全管理、项目 8 数据安全交换。8 个项目的编排按照“总体认知→外部威胁→边界防护→系统管理→数据管理→内网管理→安全接入”的顺序，与企业网络安全体系构建的思路相符，逐步引导学生构建一个完整的计算机网络安全防护图景。

本书项目 1、4、8 由浙江工商职业技术学院吕新荣老师编写，项目 3、6 由浙江工商职业技术学院陆世伟老师编写，项目 5 由太原城市职业技术学院侯小丽老师编写，项目 2 由河南建筑职业技术学院陈致远老师编写，项目 7 由广东工程职业技术学院朱珍老师编写。全书由吕新荣老师统稿。

由于编者的学识水平有限，书中难免会有不当之处，恳请读者不吝赐教，使本书得以不断完善。

编　者

2012 年 7 月

目　录

项目1 计算机网络安全认识

教学目标

最终目标	对网络安全能有一个总体的认识
促成目标	(1) 理解网络安全的含义 (2) 了解网络面临的各种威胁 (3) 了解网络安全体系 (4) 了解网络安全防护技术 (5) 熟悉网络安全涉及的道德伦理和法律、法规 (6) 注重培养学生的良好网络安全意识和道德习惯

引言

人们经常可以从各种媒体上看到有关网络安全事件的报道，这些网络安全事件包括病毒传播、黑客入侵、银行账户被盗等。作为一名相关专业的学生，在学习具体的网络安全技术之前，需要对计算机网络安全有一个整体的认识。

模块 1　网络安全典型案例分析

任务 1　典型案例 1

1.1　任务引入

分析下面两个安全事件。

事件 1：CSDN、天涯等大型网站用户密码泄漏

2011 年 12 月 21 日，国内最大的开发者社区 CSDN.NET 承认安全系统遭到黑客攻击，CSDN 数据库中的部分用户的登录名及密码遭到泄露。相同时间天涯论坛也承认网站密码泄露，被泄露的用户密码全部以明文方式保存。

CSDN 网站关于此事的官方声明中表示，泄露出来的 CSDN 明文账号数据是 2010 年 9 月之前的数据，并提醒之前注册并没有修改过密码的用户修改密码。业内人士爆料说，在网上公开的 CSDN 用户资料，相比目前互联网上被盗的众多用户数据来说只是很少的一部分，更多的数据已经被黑客转手卖钱。

事件 2：中国银行用户遭遇网银升级骗局

2011 年 1 月，许多人都收到了一条称中行网银 E 令已过期的短信，要求立即登录某网站(假冒的中国银行网站)进行升级。而实际上这是不法分子冒充中国银行网站，以中行网银 E 令(网上银行动态口令牌)升级为由实施网络诈骗。此类诈骗手法将传统的短信诈骗与钓鱼网站相结合，欺骗性更强。据《钱江晚报》报道，绍兴市民章某在接到假冒的中行网银 E 令卡升级的短信后，登录假中行网站，48 秒中内 100 万元被偷走。无独有偶，当地的魏先生、陆先生也分别被相同骗局骗走了 1700 元和 11 万元。

安全专家表示，这是一起典型的网络诈骗案，犯罪分子利用互联网和现代通信手段，冒充中国银行发送短信，以中国银行系统升级或事主办理的中行网银动态口令牌需要立即升级为由，让其登录假冒的中国银行网站并要求事主在假冒网站上输入银行卡号和密码，一旦事主按照提示进行操作，事主的网银用户名、密码及动态口令即被盗取，卡内现金也被悉数转走，同时该假冒网站立即消失。

1.2　相关知识

1. 网络安全定义

随着信息技术的飞速发展和广泛应用，计算机、网络、信息已经成为当今企业参与市场竞争的基本设施。计算机安全、网络安全、信息安全三者在内涵上已经无法区分，现在人们经常用它们之间的某一个概念来表达相关含义。

要对网络安全下一个精确的定义不是一件容易的事情，通常把网络安全理解为网络信息系统抵御意外事件或恶意行为的能力，这些意外事件或恶意行为将危及所存储、处理或传输的数据以及经由这些系统所提供的服务的机密性、完整性、可用性、不可否认性、真实性和可控性。这 6 种性质的具体含义如下。

(1) 机密性(Confidentiality)：是指保护数据不受非法截获和未经授权浏览。这一点对敏感数据的传输尤为重要，同时也是通信网络中处理用户的私人信息必须拥有的性质。

(2) 完整性(Integrity)：是指保障被传输、接收或存储的数据是完整的和未被篡改的。这一

点对保障一些重要数据的精确性尤为关键。

(3) 可用性(Availability)：是指尽管存在可能的突发事件如供电中断、自然灾害、事故或恐怖袭击等，但用户依然可以得到或使用数据，服务也处于正常运转状态。

(4) 不可否认性(Non-repudiation)：是指保证信息行为人不能事后否认曾经进行过的信息生成、签发、接收等行为。这一点在电子商务交易中非常重要，可以防止有人恶意购买后拒绝付款等行为。

(5) 真实性(Authenticity)：是指保证实体(如人、进程或系统)身份或信息、信息来源的真实性。

(6) 可控性(Controllability)：是指保证信息和信息系统的授权认证和监控管理。

2. 网络安全威胁

网络安全威胁是指可能对网络系统造成危害的不希望事故的潜在起因。

网络威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素可分为恶意和非恶意两种。环境因素包括自然界不可抵抗的因素和其他物理因素。威胁作用形式可以是对信息系统直接或间接地攻击，在保密性、完整性和可用性等方面造成损害，也可能是偶发的或蓄意的事件。

根据《信息安全风险评估规范》(GB/T 20984—2007)，网络安全威胁基于表现形式可以分为软硬件故障、物理环境影响、无作为或操作失误、管理不到位、恶意代码、越权或滥用、网络攻击、物理攻击、泄密、篡改和抵赖等。

(1) 软硬件故障：对业务实施或系统运行产生影响的设备硬件故障、通信链路中断、系统本身或软件缺陷等问题。

(2) 物理环境影响：对信息系统正常运行造成影响的物理环境问题和自然灾害。

(3) 无作为或操作失误：应该执行而没有执行相应的操作，或无意执行了错误的操作。

(4) 管理不到位：安全管理无法落实或不到位，从而破坏信息系统正常有序地运行。

(5) 恶意代码：故意在计算机系统上执行恶意任务的程序代码。

(6) 越权或滥用：通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出了破坏信息系统的行为。

(7) 网络攻击：利用工具和技术通过网络对信息系统进行攻击和入侵。

(8) 物理攻击：通过物理的接触造成对软件、硬件、数据的破坏。

(9) 泄密：将信息泄露给不应了解的他人。

(10) 篡改：非法修改信息，破坏信息的完整性，使系统的安全性降低或信息不可用。

(11) 抵赖：不承认收到的信息和所做的操作和交易。

1.3　任务实施

利用百度或谷歌检索近两年发生的重点网络安全事件，并对这些事件展开讨论。

任务 2　典型案例 2

2.1　任务引入

分析下面两个案例。

事件 1：网络空间的精确制导武器——“震网”(Stuxnet)病毒

2010 年伊朗境内的诸多工业、企业遭遇了一种极为特殊的计算机病毒袭击。知情人士称，

这种代号为“震网”的“计算机蠕虫”侵入了工厂企业的控制系统，并有可能取得对一系列核心生产设备，尤其是发电企业的关键控制权。广受西方关注的布舍尔核电站也是“震网”蠕虫的重点“关照对象”。2011 年，一种被认为是 Stuxnet 病毒的变种 Duqu 病毒开始传播，可能成为 2012 年的主要恶意软件。

Stuxnet 病毒普遍被怀疑是美国和以色列等国针对伊朗核设施展开的一次网络攻击，大家普遍担心这将开启网络战争，并引发更严重的网络恐怖活动，从而引发巨大灾难。

事件 2：美国发布《网络空间国际战略》

2011 年 5 月 6 日，美国白宫国土安全及反恐事务顾问布伦南、国务卿希拉里•克林顿、司法部长霍尔德、商务部长骆家辉、国土安全部长纳波利塔诺等政要出席了美国《网络空间国际战略》(International Strategy for Cyberspace)的发布会。这份 25 页的文件阐述了美国的网络空间战略原则，其中关于如果日后美国有可能遭遇威胁国土安全的网络攻击，可以动用军事实力反击的内容受到了全球关注。

网络空间已经成为国家重要的信息基础设施，随着物理空间和网络空间的深度融合，网络空间安全已经上升到国家安全的战略层面。网络空间将成为继陆、海、空、天后第 5 维国家竞争领域，制定我国国家网络空间战略迫在眉睫。

2.2 相关知识

1. 网络安全技术

网络安全技术是保障网络安全的重要措施之一，现有的网络安全技术包括以下内容。

(1) 防火墙技术。
(2) 加密技术。
(3) 鉴别技术。
(4) 数字签名技术。
(5) 入侵检测技术。
(6) 审计监控技术。
(7) 病毒防治技术。
(8) 备份与恢复技术。

2. 网络安全体系

网络安全是网络所处的一种状态，当组织发生变化时，网络安全状态也会发生变化，因此保障网络安全也是一个动态的过程，那种认为网络安全只要把相关设备和措施实施完毕就可以高枕无忧的想法是非常有害的。

构建网络安全体系要遵循以下原则。

1) 木桶原则

网络安全涉及方方面面，无论哪个方面薄弱，都会对整体的安全带来隐患，特别是要改变重技术轻管理的意识。

2) 多重防护原则

网络安全防护是一个系统工程，在面对复杂的网络攻击时，需要将多种防护手段有机地结合，构成多层次的防护体系。

3) 注重安全层次和安全级别

网络安全是一项防患于未然的事业，投入也非常大，保护的重点应该放在高价值的资产上，识别重要信息资产是构建网络安全体系的第一步。

4) 动态化原则

没有永远安全的网络，网络安全系统是一个动态系统，网络安全技术人员必须定期评估和完善自身的安全体系。风险评估是维护网络安全体系正常运转的一项日常基础工作。

网络安全保障问题不仅仅是技术问题，更是管理问题。据有关机构统计表明，网络与信息安全事件大约有 70%以上的问题是由管理因素造成的。“三分技术、七分管理”经常被安全专家所强调。

2.3　任务实施

通过搜索引擎检索有关“震网”病毒和美国《网络空间国际战略》的信息，讨论这些事件对我国网络空间安全的影响和应对策略。

模块 2　道德与法律

任务 1　网络安全的道德

1.1　任务引入

在美国的拉斯维加斯每年都要召开一次黑帽子(Blackhat)大会。黑帽子大会一直被公认为是信息安全领域的顶级盛会，在预测与描述未来信息安全形势的能力方面，它的权威性更是独一无二的，它汇聚了来自世界各地的企业、政府、学术界及“地下”信息安全组织的思想领袖。在这个专业与技术水平极高的平台上，黑客们向人们展示操控世界的技术。

1.2　相关知识

1. 黑客与骇客

在普通人眼里，黑客(Hacker)是一群技术高超喜欢入侵计算机获取机密的神秘人物。但从历史发展来看，真正的黑客指的是那些对计算机、网络以及各种软件技术非常感兴趣并能解决各种难题的高手。黑客有自己的精神追求，自由软件基金会创始人 Richard Stallman 说过：“出于兴趣而解决某个难题，不管它有没有，这就是黑客。”

黑客不追求金钱和破坏，追求这些的人是骇客(Cracker)，这些人强行闯入别人的系统或以某种恶意的目的干扰或破坏别人的系统。

黑客极大地推动了计算机技术的发展和普及，谱写了激动人心的黑客历史，孕育了追求自由开放创新的黑客文化，形成了特有的黑客道德。

1984 年，美国《新闻周刊》记者 Steven Levy 出版的关于黑客著作《黑客：计算机革命的英雄》，对黑客的道德伦理观进行了总结，提出了 6 条基本原则，读者可以查询相关书籍了解这 6 条原则。

2. 社会工程学

爱因斯坦说过“只有两种事物是无穷尽的——宇宙和人类智慧，但对于前者我不敢确定”。

社会工程学就是利用人类的智慧，使其他人顺从你的意愿、满足你的欲望，操作他人执行预期的动作或泄漏机密信息的一门艺术和学问。网络安全涉及防护技术、安全措施和人，而其中人永远是最薄弱的环节，再强大的加密算法也无法保护没有密码保护意识的人所管理的重要信息。

史上最有名的社会工程师是著名黑客 Kevin Mitnick，他的著作《欺骗的艺术》是关于社会工程学的经典书籍，此人后来被 FBI 逮捕并入狱(曾 3 次入狱，第 3 次入狱堪称传奇)，释放后改邪归正成为一名网络安全技术专家。

1.3 任务实施

阅读有关黑客的书籍，如 Paul Graham 著的《黑客与画家》、Kevin Mitnick 著的《欺骗的艺术》，撰写一篇关于黑客的小论文。

任务 2 网络安全的法律

2.1 任务引入

2009 年 6 月 5 日，南京市鼓楼区人民法院以非法侵入计算机系统罪，分别判处王华、龙斌、周牧等 6 名被告人 1 年至 1 年两个月不等的有期徒刑，并处高额罚金，其非法所得及作案工具均被依法没收。案件宣判后，6 名被告人均未上诉，判决于 6 月 16 日生效。据悉，此案是《刑法修正案(七)》颁布实施以来，全国法院首次适用刑法新增条款判决的黑客犯罪案件。

2008 年 5 月，江苏省一家政府网站突然出现异常情况，原因是该网站被“挂马”了，即被黑客利用网站漏洞向网页植入了恶意代码，也就是人们常说的木马程序。这样，当普通用户访问这个网页时，就会在察觉不到的情况下，同时访问另一个网址的服务器，而在这个服务器上黑客已经预置了大量木马程序。普通计算机用户只要一链接上，这些木马程序就会在不知不觉中被下载到他们的计算机中去。

经调查，这起案件的受害者多为网络游戏用户。犯罪嫌疑人通过木马程序盗窃这些用户的网游账号和密码，以此牟利。据警方介绍，在本案中兴风作浪的是“大小姐”系列木马，它共有 40 余款变种，可对几十种主流网络游戏进行盗号，相关市场占有率达 60%以上。警方最终锁定了这个犯罪团伙组织者王华、全国总代理周牧以及“大小姐”系列木马的作者龙斌。在王华的计算机中警方发现被盗的玩家账号和密码竟有两亿多个。该团伙能够认定的非法所得高达 1200 多万元。

2.2 相关知识

根据我国公安部计算机管理监察司的定义，所谓计算机犯罪，就是在信息活动领域中，利用计算机信息系统或计算机信息知识作为手段，或者针对计算机信息系统，对国家、团体或个人造成危害，依据法律规定，应当予以刑法处罚的行为。

我国《刑法》关于计算机犯罪的有关条款如下。

第二百八十五条(非法侵入计算机信息系统罪)违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处 3 年以下有期徒刑或者拘役。

第二百八十六条(破坏计算机信息系统罪)

(1) 第一款：违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处 5 年以下有期徒刑或者拘役；后果特别严重的，处 5 年以上有期徒刑。

(2) 第二款：违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

(3) 第三款：故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条(利用计算机实施的各类犯罪)利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

2009 年 2 月对第 285 条进行了修正，增加两款。

(1) 第二款：违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处 3 年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处 3 年以上 7 年以下有期徒刑，并处罚金。

(2) 第三款：提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

2.3　任务实施

阅读我国关于计算机犯罪的相关法律规定，讨论经常发生的与网络安全技术有关的行为，如同学之间传递木马或攻击工具是否属于违法行为。

项 目 小 结

本项目包括两个模块，第 1 个模块通过分析两个典型的网络安全案例来学习网络安全的基本概念，并通过分析讨论的方式探讨网络安全的危害性和紧迫性；第 2 个模块通过典型的网络安全犯罪案例来学习与计算机安全和犯罪有关的道德和法律，引导学生树立正确的网络安全道德和法律意识，避免走入误区。

思 考 练 习

一、选择题

1. 计算机网络安全的主要含义是指(　　)。

A. 网络中设备环境的安全　　B. 网络使用者的安全

C. 网络中信息的安全　　D. 网络的财产安全

2. 以下(　　)不是保证网络安全的要素。

A. 信息的保密性　　B. 发送信息的不可否认性

C. 数据交换的完整性　　D. 数据存储的唯一性

3．以下属于网络安全威胁的有(　　)。

A．断电　　B．管理不到位　　C．泄密

D．盗窃　　E．篡改

4．网络安全技术包括(　　)。

A．防火墙技术　　B．加密技术　　C．备份技术

D．病毒防治　　E．入侵检测技术

5．构建网络安全技术需要遵循的原则有(　　)。

A．木桶原则　　B．多重防护原则

C．注重安全层次和安全级别　　D．动态化原则

6．我国《刑法》定义的计算机犯罪有(　　)。

A．非法侵入计算机信息系统罪　　B．破坏计算机信息系统罪

C．利用计算机实施的各类犯罪　　D．非法闯入计算机罪

7．下面(　　)行为构成计算机犯罪。

A．侵入我国某地方政府的网站服务器　　B．将木马程序传给 QQ 好友

C．在实验室计算机上编写木马程序　　D．将网站信息复制到自己的计算机上

二、填空题

1．_____是指保证信息和信息系统的授权认证和监控管理。

2．_____是指可能对网络系统造成危害的不希望事故的潜在起因。

3．_____是维护网络安全体系正常运转的一项日常基础工作。

4．一个组织的网络安全最薄弱环节往往在于_____。

5．违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处_____以下有期徒刑或者_____。

三、简答题

1．简述网络安全的定义。

2．根据作用形式，网络安全威胁可以分为哪些种类？

3．简述社会工程学的定义及其特点。

4．什么是计算机犯罪？

四、实践讨论题

1．观看一部与计算机犯罪有关的电影，与同学交流观后感。

2．从互联网上检索有关著名黑客的传奇故事，与同学探讨黑客对 IT 技术发展的影响。

3．从互联网上检索国内外与计算机犯罪有关的法律条例以及法律专家的解读，与同学探讨在学习网络安全技术的同时如何避免触发法律。

项目2 网络病毒防范

教学目标

最终目标	能防范和识别常见的网络病毒
促成目标	(1) 理解网络病毒的危害性 (2) 学会判断常见网络病毒引起的现象 (3) 理解蠕虫病毒的传播机制 (4) 掌握蠕虫病毒的防范策略 (5) 理解 USB 病毒传播机制 (6) 掌握 USB 病毒的防范策略 (7) 培养学生提高防范病毒的安全意识

引言

网络病毒是一种新型病毒，它的传播媒介不再是移动式载体，而是网络通道，这类病毒的传染能力更强，破坏力更大。同时有关调查显示，通过电子邮件和网络进行病毒传播的比例正逐步攀升，它们给人们的工作和生活带来了很多麻烦。本项目通过选取蠕虫病毒、USB 病毒等一些常见病毒进行分析并提出若干防范机制，以此提高防毒意识。

模块 1　蠕虫病毒防范

任务 1　蠕虫病毒分析

1.1　任务引入

随着网络的普及，网络给人们的生活和工作带来了很多的方便，但是由于人们的安全意识不够强，从而经常遭受各种病毒的攻击，导致很多悲剧发生。病毒攻击中蠕虫病毒攻击是比较常见的，产生的破坏力有时也很大，比如 1988 年一个由美国 Cornell 大学研究生莫里斯编写的蠕虫病毒蔓延造成了数千台计算机停机，蠕虫病毒开始现身网络，而后来的红色代码、尼姆达病毒疯狂的时候，造成几十亿美元的损失。这些蠕虫病毒通过分布式网络来扩散、传播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁。那么如何来识别和认识这种病毒呢？

1.2　相关知识

1. 蠕虫病毒基本特点

网络蠕虫是无需计算机使用者干预即可运行的独立程序，是一种通过网络传播的恶性病毒，它通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。可以说蠕虫病毒是一种常见的计算机病毒，与一般病毒不同，蠕虫病毒不需要将其自身附着到宿主程序，是一种独立智能程序。它利用网络进行传播并能够自我复制，爆发时消耗大量的系统资源，使其他程序运行减慢甚至停止，最后导致系统和网络瘫痪。其传播方式为两类：一类是利用系统漏洞主动进行攻击；另一类是通过网络服务器传播。目前企事业单位中员工计算机水平参差不齐，几乎所有的计算机都接入到园区网络中，网络应用复杂，一旦有计算机感染蠕虫病毒就快速地在园区网络中传播，并利用系统漏洞完成自我复制，导致园区网中很多计算机感染蠕虫病毒。轻则影响园区内局域网网络安全与稳定地运行，重则导致园区网络瘫痪，用户无法访问校园网内外资源。

2. 蠕虫的程序结构及工作流程

蠕虫病毒的程序结构通常包括 3 个模块：①传播模块，负责蠕虫的传播，它可以分为扫描模块、攻击模块和复制模块 3 个子模块，其中，扫描模块负责探测存在漏洞的主机，攻击模块按漏洞攻击步骤自动攻击找到的对象，复制模块通过原主机和新主机交互将蠕虫程序复制到新主机上并启动；②隐藏模块，侵入主机后，负责隐藏蠕虫程序，防止被用户发现；③目的功能模块，实现对计算机的控制、监视或破坏等。

根据蠕虫病毒的程序，其工作流程可以分为漏洞扫描、攻击、传染、现场处理 4 个阶段，首先蠕虫程序随机(或在某种倾向性策略下)选取某一段 IP 地址，接着对这一地址段的主机进行扫描，当扫描到有漏洞的计算机系统后，将蠕虫主体迁移到目标主机。然后，蠕虫程序进入被感染的系统，对目标主机进行现场处理。同时，蠕虫程序生成多个副本，重复上述流程。各个步骤的繁简程度也不同，有的十分复杂，有的则非常简单。工作流程如图 2-1 所示。

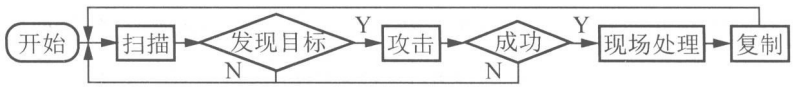

图 2-1　蠕虫病毒的工作流程

3. 蠕虫病毒的基本特征

蠕虫病毒具有如下基本特征。

(1) 蠕虫病毒具有自我复制的能力。

(2) 蠕虫病毒具有很强的传播性。病毒需要传播，电子邮件病毒的传播无疑是通过电子邮件传播的。对于 Outlook 来说，地址簿的功能相当不错，可是也给病毒的传播打开了方便之门。大多数通过 Outlook 传播的电子邮件病毒是向地址簿中存储的电子邮件地址发送内容相同的脚本附件完成的。

(3) 蠕虫病毒具有一定的潜伏性。对于“脚本”语言，要使病毒潜伏并不是很难的一件事，因为这种语言并不是面向对象的可视化编程，自然就不存在窗体，所以可以免去隐藏窗体的麻烦。

(4) 蠕虫病毒具有特定的触发性。

(5) 蠕虫病毒具有很大的破坏性。

蠕虫病毒的危害会造成全球经济的巨大损失，这些损失可能远远大于地震、台风甚至火山喷发等自然灾害所造成的损失。表 2-1 列举了比较典型的几种蠕虫病毒发作后带来的经济损失。

表 2-1　典型蠕虫病毒攻击举例

病毒名称	发作时间	造成的损失
莫里斯蠕虫	1988 年 11 月	6000 多台计算机停机，直接经济损失达 9600 万美元
美丽杀手	1999 年 4 月	政府部门和一些大公司紧急关闭了网络服务器，经济损失超过 12 亿美元
爱虫病毒	2000 年 5 月	众多用户计算机被感染，损失超过 100 亿美元
红色代码	2001 年 7 月	网络瘫痪，直接经济损失超过 26 亿美元
求职信	2001 年 12 月	大量病毒邮件堵塞服务器，损失达数百亿美元
SQL 蠕虫王	2003 年 1 月	网络大面积瘫痪，银行自动提款机运作中断，直接经济损失超过 26 亿美元
冲击波	2003 年 7 月	大量网络瘫痪，造成了数十亿美金的损失
MyDoom	2004 年 1 月	大量的垃圾邮件，攻击 Sco 和微软网站，给全球经济造成了 300 多亿美元的损失

4. 蠕虫的行为特征

蠕虫能自我繁殖，蠕虫在本质上已经演变为黑客入侵的自动化工具，当蠕虫被释放后，从搜索漏洞到利用搜索结果攻击系统，再到复制副本，整个流程全由蠕虫自身主动完成；任何计算机系统都存在漏洞，蠕虫利用系统的漏洞获得被攻击计算机系统的相应权限，使之进行复制和传播的过程成为可能。这些漏洞是各种各样的，有的是操作系统本身的问题，有的是应用服务的问题，有的是网络管理人员的配置问题。正是由于漏洞产生原因的复杂性，导致各种类型的蠕虫泛滥；造成网络拥塞，在扫描漏洞主机的过程中，判断其他计算机是否存在，判断特定应用服务是否存在，判断漏洞是否存在等，这不可避免地会产生附加的网络数据流量。同时蠕虫副本在不同计算机之间传递，或者向随机目标发出的攻击数据都不可避免地会产生大量的网络数据流量。即使是不包含破坏系统正常工作的恶意代码的蠕虫，也会因为它产生了巨量的网