新世纪职业教育应用型人才培养培训创新教材

卢江兴 主编

计算机网络攻防实训

清华大学出版社

新世纪职业教育应用型人才培养培训创新教材

卢江兴 主编

计算机网络攻防实训

清华大学出版社
北京

内 容 简 介

本书利用虚拟机软件，搭建虚拟机实训环境，精选10个完整的网络攻防案例，包括：WDX远程溢出、手工入侵共享连接主机、Serv-U 5.0远程溢出、网站挂马、IDQ提权、Cookies欺骗上传、社工欺骗、MS SQL远程溢出、Windwos 2003溢出、ShellCode编程。案例虽然以Windows 2000为主要攻击对象，但其手法、原理对其他操作系统，包括Windows 2008、Linux、UNIX等系统的攻防也有借鉴作用。设计的每个案例尽可能代表一种攻防技术，以攻防为主线，一个案例就是对虚拟机的一次完整攻击，着重展现案例入侵的完整过程，分析其中使用的手法、思路，每个案例均配有教学视频，真正做到项目教学，方便教学实施及自学研究。

本书适合中、高职院校计算机相关专业学生及对计算机安全有爱好的社会读者。

图书在版编目（CIP）数据

计算机网络攻防实训/卢江兴主编. --北京：清华大学出版社，2015
新世纪职业教育应用型人才培养培训创新教材
ISBN 978-7-302-38814-2

Ⅰ. ①计… Ⅱ. ①卢… Ⅲ. ①计算机网络－安全技术－中等专业学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2014)第301084号

责任编辑：张　弛
封面设计：王跃宇
责任校对：刘　静
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795764

印 装 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：11　　**字　　数**：265千字
版　　次：2015年2月第1版　　**印　　次**：2015年2月第1次印刷
印　　数：1～2000
定　　价：25.00元

产品编号：062052-01

前言
FOREWORD

在职业教育中，网络攻防课程难上，主要体现在：资料零散，不知道要从什么地方开始学习，感觉很茫然；没有具体任务，没有实践的机会；没有自主安装相关实验系统以及软件的机会；没有足够的时间进行实验；理论偏多，攻防实践效果不明显，实验结果难以理解等。

在网络安全中，攻防是对立而统一的，只有知道如何攻，才能更好地防守。基于“授之以渔”的理念，本书不以黑防工具的用法介绍为主，而是着重展现每一个案例入侵的完整过程，分析其中使用的手法、思路。

本书采用案例教学法，贯彻以学生为中心的教学思想。搭建虚拟机实训环境，精选10个完整的网络攻防案例，包括：WDX远程溢出、手工入侵共享连接主机、Serv-U 5.0远程溢出、网站挂马、IDQ提权、Cookies欺骗上传、社工欺骗、MS SQL远程溢出、Windows 2003溢出、ShellCode编程。案例虽然以Windows 2000为主要攻击对象，但其手法、原理对其他操作系统，包括Windows 2008、Linux、UNIX等系统的攻防也有借鉴作用。设计的每个案例尽可能代表一种攻防技术，以攻防为主线，从实验环境建立到攻击实施，对案例中涉及的相关计算机安全知识进行阐述。

每个案例均包含以下六部分的内容。

项目描述——对整个案例进行简述。

漏洞描述——对案例中涉及的漏洞进行说明。

项目分解——对项目的简单分析。

项目实训——完成项目实训的完整过程。

项目小结——对完成项目进行的简单评述。

知识链接——作为开阔视野而提供的阅读材料。

每个案例均提供操作视频、攻防实训需要的工具，由于所有工具均来源于互联网，编者虽尽全力也不能保证所有工具无毒、无漏洞。为此，建议实训时应断开与真实网络的连接，以避免造成不必要的损失。建议教学课时为40课时。

本书不是教授黑客技术的教材，期望通过阅读本书而能够入侵其他的计算机是不现实的。通过阅读本书，读者可以了解黑客入侵的过程、手法，进而建立安全防范意识及提高安全防范能力。由于受搭建实训环境及实训结果易见性两方面的限制，本书未能包括交换机、路由器、无线网络等与硬件密切相关的内容。

书中案例攻击的网站或系统为旧版本文件，作为教学素材，只用于演示安全相关概念，并无对原作者不敬之意。

由于编者水平有限，疏漏之处在所难免，敬请广大读者批评指正。编者邮箱：20920139@qq.com。

编　者

2014年8月

目 录
CONTENTS

项目1

概　述

1.1 信　息

“信息”一词在英文、法文、德文、西班牙文中均是“information”，日文中为“情报”，我国台湾称为“资讯”，我国古代用的是“消息”。作为科学术语最早出现在哈特莱(R. V. Hartley)于1928年撰写的《信息传输》一文中。20世纪40年代，信息的奠基人香农(C. E. Shannon)给出了信息的明确定义，此后许多研究者从各自的研究领域出发，给出了不同的定义。具有代表意义的表述如下。

香农认为“信息是用来消除随机不确定性的东西”，这一定义被人们看做经典性定义并加以引用。

控制论创始人维纳(Norbert Wiener)认为“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称”，它也被作为经典性定义加以引用。

经济管理学家认为“信息是提供决策的有效数据”。

根据对信息的研究成果，科学的信息概念可以概括如下。

信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。

信息是客观事实的可通信的知识，具有以下几个基本特征。

(1) 信息是客观世界各种事物的特征(时间、地点、程度、方式等)的反映。

(2) 信息是可以通信的。

(3) 信息形成知识。

(4) 信息是有价值的，需要进行保护。

(5) 信息的价值＝利用信息所获得的收益－获得信息所花费的成本。

1.2 信息安全的定义

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断。信息安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权复制和所寄生系统的安全性。信息安全的根本目的就是使内部信息不受外部威胁，因此信息通常要加密。

为保障信息安全，要求有信息源认证、访问控制，不能有非法软件驻留，不能有非法操作。

国际标准化组织(ISO)对信息安全的定义为：为数据处理系统建立和采用的技术与管理的安全保护，保护计算机硬件、软件和数据不因偶然的和恶意的原因遭到破坏、更改和泄露。

这个定义描述了三方面的内容：①保护网络系统的硬件、软件、数据；②防止系统和数据遭到破坏、更改、泄露；③保证系统连续、可靠、正常地运行，服务不中断。

从广义上讲，涉及网络信息的保密性、完整性、可用性、真实性、可控性的相关技术和理论都是信息安全研究的内容。

主要从提高技术及强化内部管理两个方面加强安全防范。大多数的安全事件均是由内部人员发起的，例如，2013 年的斯诺登“棱镜”事件，虽然对于全世界而言，斯洛登披露了美国政府的监听丑闻，但是从美国安全局的角度出发，就是发生了非常严重的安全事件，而这个事件是由内部人员引起的。

“棱镜”事件(PRISM)

2013 年 6 月，前中情局职员爱德华·斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，并告知媒体何时发表。

6 月 5 日，英国《卫报》扔出一颗舆论炸弹：美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。6 月 6 日，美国《华盛顿邮报》披露称，过去 6 年间，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果、雅虎等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。

美国国家安全局与联邦调查局参与了这项代号为“棱镜”的项目，与政府机构合作的九家互联网公司分别是：微软、雅虎、谷歌、Facebook、PalTalk、美国在线、Skype、YouTube、苹果。《华盛顿邮报》获得的文件显示，美国总统的日常简报内容部分来源于此项目，该工具被称做获得此类信息的最全面方式。报道刊出后外界哗然。保护公民隐私组织予以强烈谴责，表示不管奥巴马政府如何以反恐之名进行申辩，不管多少国会议员或政府部门支持监视民众，这些项目都侵犯了公民的基本权利。

1.3 信息安全的目标

信息安全涉及的范围很大，包括如何防范商业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制(数字签名、消息认证、数据加密等)，其中任何一个安全漏洞都可以威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

所有的信息安全技术都是为了达到一定的安全目标，其核心包括保密性、完整性、可用性、可控性和不可否认性。

保密性(Confidentiality)是指阻止非授权的主体阅读信息。它是信息安全从诞生就具有的特性，也是信息安全主要的研究内容之一。通俗地说，就是说未授权的用户不能够获取敏感信息。对纸质文档信息，只需保护好文件，不被非授权者接触即可。而对计算机及网络环境中的信息，不仅要制止非授权者对信息的阅读，也要阻止授权者将其访问的信息传递给非授权者，以致信息被泄露。

完整性(Integrity)是指防止信息被未经授权的篡改,即保持信息原始的状态,使信息保持其真实性。如果信息被蓄意地修改、插入、删除等,形成虚假信息将带来严重的后果。

可用性(Availability)是指授权主体在需要信息时能及时得到服务。可用性是在信息安全保护阶段对信息安全提出的新要求,也是在网络空间中必须满足的一项信息安全要求。

可控性(Controlability)是指对信息和信息系统实施安全监控管理,防止非法利用信息和信息系统。

不可否认性(Non-repudiation)是指在网络环境中,信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为。

信息安全的保密性、完整性和可用性主要强调对非授权主体的控制,可控性和不可否认性是对授权主体的控制,实现对保密性、完整性和可用性的有效补充,主要强调授权用户只能在授权范围内进行合法的访问,并对其行为进行监督和审查。

除了上述的信息安全"五性"外,还有信息安全的可审计性(Audiability)、可鉴别性(Authenticity)等。信息安全的可审计性是指信息系统的行为人不能否认自己的信息处理行为。与信息交换过程中的不可否认性相比,可审计性的含义更宽泛一些。信息安全的可鉴别性是指信息的接收者能对信息的发送者的身份进行判定,它也是一个与不可否认性相关的概念。

简单地说,信息安全就是要实现以下几个目标。

(1) 进不来——只有得到授权的用户才能正常使用系统。

(2) 拿不走——即使非授权用户能够进入系统,也不能复制相关信息。

(3) 看不懂——即使非授权用户能够复制相关信息,但也因为信息被加密而看不懂。

(4) 改不了——因为信息被加密,从而不能正常修改;或者能修改,但会被发现。

(5) 跑不了——入侵者会被发现。

(6) 可审查——日志系统会对入侵者的行为进行记录。

1.4 实施信息安全的原则

信息安全具有相对性,只有相对安全,没有绝对安全的系统,随着时间的变化,原来安全的系统会变得不安全,具有时效性;信息安全具有配置相关性,日常管理中不同的软件、硬件配置会引入新的安全问题;信息安全具有攻击不确定性:攻击发起的时间、攻击者、目标、发起地点都具有不确定性;信息安全具有复杂性:信息安全是一项系统工程,需要技术和非技术手段,涉及安全管理、教育、立法等方面的内容。

为了达到信息安全的目标,各种信息安全技术的使用必须遵守以下一些基本的原则。

最小化原则。受保护的敏感信息只能在一定范围内被共享,履行工作职责和职能的安全主体,在法律和相关安全策略允许的前提下,为满足工作需要仅被授予其访问信息的适当权限。敏感信息的"知情权"一定要加以限制,是在"满足工作需要"前提下的一种限制性开放。可以将最小化原则细分为知所必须(need to know)和用所必须(need to use)的原则。

分权制衡原则。在信息系统中,对所有权限应该进行适当的划分,使每个授权主体只能拥有其中的一部分权限,使它们之间相互制约、相互监督,共同保证信息系统的安全。如果一个授权主体分配的权限过大,无人监督和制约,就隐含了"滥用权力"、"一言九鼎"的安全

隐患。

安全隔离原则。隔离和控制是实现信息安全的基本方法，而隔离是进行控制的基础。信息安全的一个基本策略就是将信息的主体与客体分离，按照一定的安全策略，在可控和安全的前提下实施主体对客体的访问。

在这些基本原则的基础上，人们在生产实践过程中还总结出一些实施原则，它们是基本原则的具体体现和扩展，包括：整体保护原则、谁主管谁负责原则、适度保护的等级化原则、分域保护原则、动态保护原则、多级保护原则、深度保护原则和信息流向原则等。

1.5 信息与网络安全组件

信息安全组件包括安全操作系统、应用系统、防火墙、网络监控、安全扫描、信息审计、通信加密、灾难恢复、网络反病毒等，如图 1-1 所示，每一个组件只能完成其中部分功能，而不能完成全部功能。

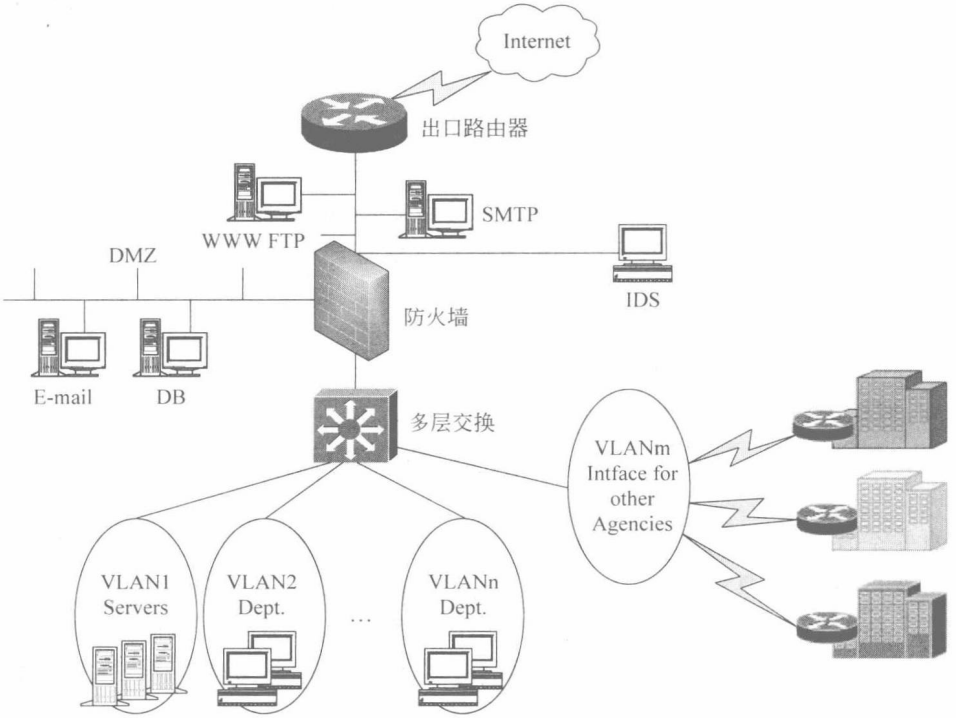

图 1-1

常见网络安全技术有以下几种。

1. 防火墙

防火墙(FireWall)是指在计算机和它所连接的网络之间设置的硬件或软件，它也可以设置在两个或多个网络之间，所有进出网络的数据流都要经过防火墙。防火墙按照管理员预先定义好的规则对数据流的进出进行控制。通过防火墙可以对网络间的通信进行扫描，从而保证网络和计算机的安全。

2. 加密

加密(Encryption)是指通过对信息加以重新组合,使得信息只能被通信双方解码并还原的一种手段。传统的加密是一种以密钥为基础的对称加密码,即用户对信息进行加密和解密时使用相同的密钥。

3. 身份认证

防火墙是系统的第一道防线,用以防止非法数据的侵入,而身份认证(Authentication)的作用则是阻止非法用户。有多种方法来鉴别一个用户的合法性,密码是最常用的。但由于有许多用户采用了很容易被猜到的单词或短语作为密码,该方法经常失效。其他方法包括对人体生理特征(如指纹)的识别、智能 IC 卡和 USB 盘。

4. 数字签名

数字签名(Digital Signture)是指通过一个单向函数,对要传送的信息进行处理,得到用以认证信息来源并核实信息在传送过程中是否发生变化的一个字符串。数字签名能确定信息来源并能检测信息是否被篡改,而且,将数字签名用于存储的数据或程序时,可以验证数据或程序的完整性。

5. 内容检查

虽然有防火墙、加密、身份认证和数字签名,但依然会遭到病毒的攻击。有些病毒通过电子邮件或者用户下载的 ActiveX 和 Java 小程序(Applet)进行传播,带有病毒的 Applet 被激活后,它又可以自动下载其他 Applet。现在比较常见的反病毒软件都可以清除电子邮件病毒,而对于 ActiveX 和 Applet 病毒也提供了一些方法,如完善防火墙,使其能对 Applet 的运行进行监控,或者可以给 Applet 加上标签,使用户知道它们的来源。

1.6 信息安全面临的威胁简介

据报道,微软自身的 IT 基础设施,每天都遭受超过 4 000 次的来自全世界的攻击。微软的操作系统及软件受到各种补丁的困扰,从漏洞发现到打上补丁期间,所有的计算机都受到威胁。历史上,对微软系统软件进行攻击,并产生较大影响的有 Nimda、SQL Slammer、Welchin/Nachi、Blaster 等病毒或蠕虫。除此以外,广大的计算机用户还受到间谍软件、钓鱼网站、僵尸网络等的威胁和影响,88%的 PC 有病毒、1/3 的邮件是垃圾邮件。

网络攻击的方法层出不穷,常见的网络安全攻击手段有密码攻击、网络端口扫描、网络监听、拒绝服务、缓冲区溢出、IP 欺骗、电子邮件攻击等。

密码攻击又称为口令攻击,常见的密码攻击有两种:蛮力攻击和猜测攻击。用户在设置操作系统的账户密码时,通常会采用一种容易记忆的方式进行密码设置,如将其设置成自己的生日或电话号码,甚至设置为空,这就给攻击者提供了可乘之机,通过对用户信息的分析,攻击者很可能猜测出密码。

网络端口扫描可以说是网络攻击的第一步。一个端口就是一个潜在的通信通道,也是一个入侵通道。网络端口扫描通过连接远程目标不同的端口,并记录目标给予的回答,对截获的数据包进行分析,从而得到关于目标主机的有用信息。通过扫描可以发现一个主机或网络,了解正在运行在这台主机上的服务,并查找这些服务的漏洞。

网络监听又叫网络嗅探，这是较常使用的一类攻击方法。当信息在网络上以明文形式传输时，就可以使用这种方法进行攻击。只要将网络接口设置为监听模式，就可以源源不断地截获网络上传输的信息。

拒绝服务是指攻击者利用系统的缺陷，通过执行一些恶意的操作，占据大量的系统资源，从而使合法的网络用户不能及时得到应得的服务或系统资源。这种攻击方式常常会导致计算机或网络不能正常工作，拒绝服务攻击的最本质的特点是延长服务等待时间。当服务等待时间超过某个阈值时，用户可能会不能忍受长时间的等待而放弃服务。与其他多数攻击不同，拒绝服务不是为了获取网络或网络上信息的访问权，而是使计算机或网络不能提供正常的服务。

缓冲区溢出是指不考虑缓冲区中分配的数据块的大小，而把一个超过缓冲长度的字符串复制到缓冲区中，导致数据超界，结果覆盖了老的堆栈数据。缓冲区溢出广泛存在于各种操作系统、应用软件中，是一种普遍存在、非常危险的漏洞。随着技术的发展，缓冲区溢出逐渐成为最有效的一种攻击技术，缓冲区溢出攻击成功时，入侵者可能会获得目标主机的部分或全部控制权。

IP 欺骗可以说是一台主机冒充另外一台主机的 IP 地址，与其他设备通信，从而达到某种目的。

电子邮件攻击主要有两种表现：一是电子邮件轰炸，通常又称为邮件炸弹，它是指攻击者使用伪造的 IP 地址和电子邮件地址向同一电子邮件信箱发送数以千计的内容相同的垃圾邮件，致使受害人的电子邮箱被“炸”，严重者可能会对电子邮件服务器操作系统造成危险，甚至瘫痪；二是电子邮件欺骗，攻击者伪装成系统管理员，给用户发送邮件要求用户修改密码或者在看似正常的附件中加载病毒或其他木马程序。

1.7 网络入侵常规步骤

从 1940 年开始计算，黑客有以下的表现形态。20 世纪四五十年代：为撰写软件和玩弄各种程序设计技巧为乐；六七十年代：具有高度创造力和知识的计算机天才；80 年代后：具有探索、创新精神的和怀有恶意的攻击者；当代：越来越组织化、行动公开化、攻击频繁化、情况复杂化。

综观与网络安全相关的事件可以发现，自 1980 年开始，对计算机系统发起攻击的技术、手法越来越复杂，自动化程度越来越高；而入侵者能够成功入侵计算机系统所要求的技术水平越来越低，如图 1-2 所示。一个低水平的入侵者只要获得其他高水平入侵者制作的工具，同样可以成功入侵目标计算机系统，通常将这样的入侵者称为“脚本小子”。

无论是哪种类型的入侵者，要对目标系统进行攻击，通常会采用与图 1-3 所示的步骤相类似的步骤。

具体每一种漏洞的入侵，与上述步骤大致相同。作为防御方法，可以针对以上 7 个步骤，阻碍其顺利执行，从而使得攻击过程难以继续进行。例如，Windows 系统可以通过修改系统信息，使入侵者误认为目标是 UNIX 系统，使得入侵者得到错误信息，从而提高了入侵难度；可以通过关闭无用服务，减少对外服务的端口。

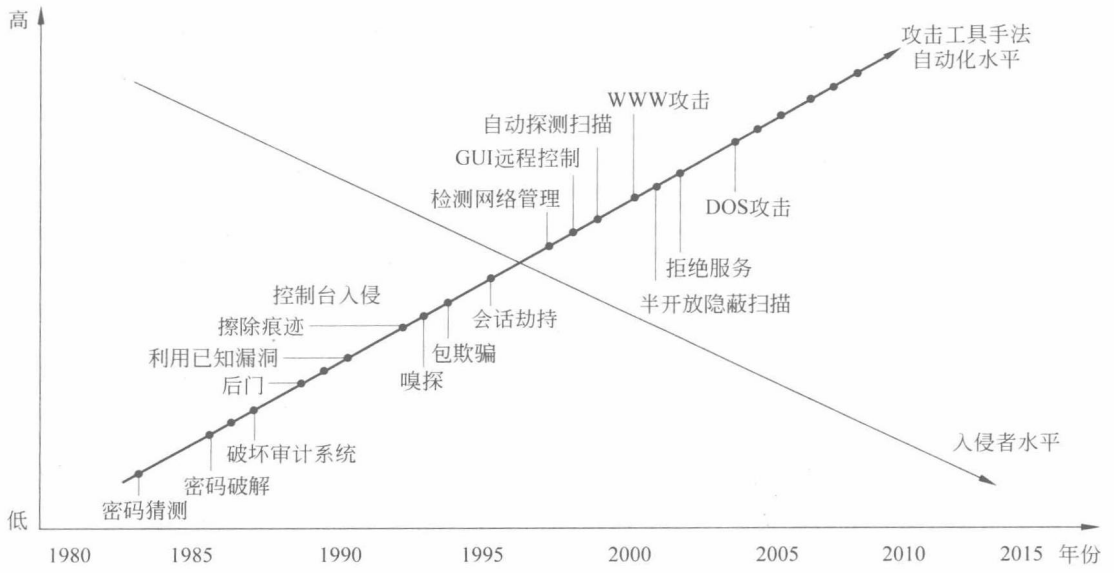

图 1-2

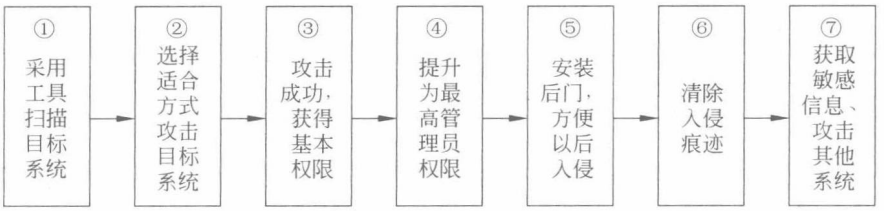

图 1-3

1.8 信息安全法律法规简介

1. 日常行为道德规范

随着现代科技的不断进步，网络已经成为必不可少的沟通、学习、工作的渠道。网络在人们的生活中充当着越来越重要的角色，人们的生活也越来越离不开网络。网络是一把锋利的“双刃剑”，在提供了便捷的同时，也对我国政治安全和文化安全构成了严重威胁。如今，在网络中出现的道德问题日益凸显。

目前比较严重的网络道德失范行为主要有以下几种。

（1）网络犯罪。一些“黑客”时常会非法潜入网络进行恶意破坏，蓄意窃取或篡改网络用户的个人资料，利用网络赌博，甚至盗窃电子银行款项。通过网络传播侵权或违法的信息等网络犯罪行为日增，互联网已成为不法分子犯罪的新领域。

（2）色情和暴力席卷而来。信息内容具有地域性，而互联网的信息传播方式则是全球性、超地域的，使得色情和暴力等问题变得突出起来。由于互联网是全球共享的，这就使得色情信息和暴力情节能够无障碍地在世界范围内传播。网络成为色情和暴力媒介，提供色情资料，灌输暴力思想，从而导致与传统优良文化道德相冲突。由于文化传统、社会价值观和社会制度不同，它对我国的危害更加严重。

(3) 网络文化侵略。互联网信息环境的开放性,使多元文化、多元价值在网上交汇。近年来,一些西方发达国家凭借网上优势,倾销自己的文化,宣扬西方的民主、自由和人权观念。这就加剧了国家之间、地区之间道德和文化的冲突,对我国的精神文明建设构成干扰和冲击。

(4) 破坏国家安全。世界上存在着对立的政治制度和意识形态,并不是到处充满善意,一些国家通过互联网发布恶意的反动政治信息,散布谣言,利用信息"炸弹"攻击他国,破坏其国家安全,甚至出于一定的政治目的,突破层层保密网,直接对其核心的系统中枢进行无声无息的破坏,达到不可告人的目的。

加强网络监管,不仅需要相关的法制建设,对网络造谣、传谣等违法行为进行法制化;还需加强网络技术管理,通过技术手段对违法行为进行打击;更重要的是要加强网络道德教育。

道德是由一定的社会组织借助于社会舆论、内心信念、传统习惯所产生的力量,使人们遵从道德规范,达到维持社会秩序、实现社会稳定目的的一种社会管理活动。在传统现实社会中形成的道德及其运行机制在网络社会中并不完全适用。不能为了维护传统道德而拒斥虚拟空间闯入生活,也不能听任网络道德处于失范无序状态,或消极地等待其自发的道德运行机制的形成。必须通过分析网络社会道德不同于现实社会生活中的道德的新特点,提出新的道德要求,加快网络道德的引导、宣传和推广,倡导道德自律。网络道德建设,需要加强政府的监管,加强网络道德教育,加强网络法制建设,多管齐下,净化网络环境,让不文明在网络上无处遁形。

2. 我国目前的网络信息安全法律法规体系介绍

网络安全问题成为社会各方面日益关注的一个热点问题。不同部门的有关人士在信息安全保障方面做了很多努力,并积累了丰富的经验。计算机科学技术领域的专家、学者从各自的专业角度,通过理论研究、技术创新、产品开发等途径,尝试着解决计算机、通信网络方面的信息安全问题;国家有关行政部门通过颁布一系列的法规和规章制度,来加强信息安全管理,协调缓解因信息安全问题而带来的矛盾;法律界的有关人士也开始讨论信息安全立法的意义和可行性。可见,对网络信息安全问题通过立法手段加以解决,产生这个想法并逐渐加深对问题的认识和理解,要有一个过程。对信息安全立法问题的认识是沿着技术—技术+管理—法律规范的发展路线逐步提高的。

2003 年下发的《关于加强信息安全保障工作的意见》(中办发[2003]27 号)是目前我国信息安全保障方面的一个纲领性文件。在此之前出台的法律法规主要分为两大类。

(1) 相关法规

1982 年 8 月,网络安全写入《中华人民共和国商标法》。

1984 年 3 月,网络安全写入《中华人民共和国专利法》。

1988 年 9 月,网络安全写入《中华人民共和国保守国家秘密法》。

1989 年,公安部发布了《计算机病毒控制规定(草案)》。

1991 年,国务院常务会议通过《计算机软件保护条例》。

1993 年 9 月,网络安全写入《中华人民共和国反不正当竞争法》。

1994 年 2 月,国务院发布《中华人民共和国计算机信息系统安全保护条例》。

1996 年 2 月,国务院发布《中华人民共和国计算机信息网络国际联网管理暂行规定》。

1997年5月，国务院信息化工作领导小组制定了《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》。

1997年，国务院信息化工作领导小组发布《我国互联网络域名注册暂行管理办法》、《我国互联网络域名注册实施细则》。

1997年，原邮电部出台《国际互联网出入信道管理办法》。

2000年，《互联网信息服务管理办法》正式实施。

2000年11月，国务院新闻办公室和信息产业部联合发布《互联网站从事登载新闻业务管理暂行规定》。

2000年11月，信息产业部发布《互联网电子公告服务管理规定》。

(2) 相关法律

1988年9月，第七届全国人民代表大会常务委员会第三次会议通过的《中华人民共和国保守国家秘密法》第三章第十七条提出："采用电子信息等技术存取、处理、传递国家秘密的办法，由国家保密部门会同中央有关机关规定。"

1997年10月，我国第一次在修订刑法时增加了计算机犯罪的罪名。

为规范互联网用户的行为，2000年12月，九届全国人大常委会通过了《全国人大常委会关于维护互联网安全的决定》。

此外，我国还缔约或者参与了许多与计算机相关的国际性的法律法规，如《成立世界知识产权组织公约》、保护文学艺术作品的《伯尔尼公约》、《世界版权公约》等。

思考题

1. 实施信息安全的主要目标是什么？
2. 简述网络攻击的一般步骤。