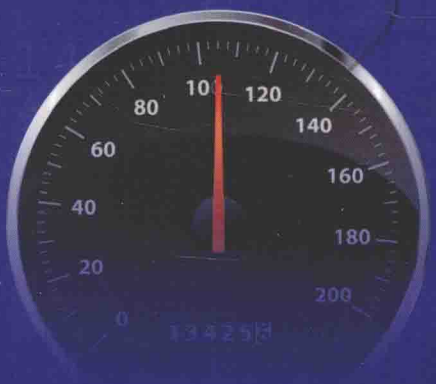
网信干部培训辅导丛书

网络安全测评
培训教程

中国网络空间研究院
中国网络空间安全协会 ◎ 编著



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

网信干部培训辅导丛书

网络安全测评
培训教程

中国网络空间研究院
中国网络空间安全协会 ◎ 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全测评培训教程 / 中国网络空间研究院，中国网络空间安全协会编著. -- 北京 : 人民邮电出版社，2016.10
（网信干部培训辅导丛书）
ISBN 978-7-115-42912-4

Ⅰ. ①网… Ⅱ. ①中… ②中… Ⅲ. ①网络安全－技术培训－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2016)第207903号

内 容 提 要

本书分四部分共10章内容。其中，第一部分（第1章、第2章）介绍信息安全测评思想和方法；第二部分（第3章～第5章）介绍安全测评的主要技术和实施流程；第三部分（第6章～第8章）介绍威胁识别、脆弱性识别及风险分析等；第四部分（第9章、第10章）介绍具体安全测评案例以及国内外该领域的最新进展。

本书旨在为全国网信干部提供理论指南、实践指导和趋势指引，也可以作为从事网络安全测评研究、实践和管理等各类专业人士的培训教材。

◆ 编　　著　中国网络空间研究院　中国网络空间安全协会
责任编辑　邢建春
执行编辑　肇　丽
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：11.5　　2016年10月第1版
字数：280千字　　2016年10月河北第1次印刷

定价：59.00元

读者服务热线：(010) 81055488　印装质量热线：(010) 81055316
反盗版热线：(010) 81055315

序　言

2014 年 2 月，中央成立了由习近平总书记任组长的中央网络安全和信息化领导小组，统筹协调各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。习近平总书记明确指出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，没有网络安全就没有国家安全，没有信息化就没有现代化”“建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍”。

2015 年 6 月，“网络空间安全”成为一级学科，把网络安全人才培养提到了一个新的战略高度。2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上明确指出：“要聚天下英才而用之，为网信事业发展提供有力人才支撑。网络空间的竞争，归根结底是人才竞争”。2016 年 7 月，国家发布《国家信息化发展战略纲要》，指出：“优化人才队伍，提升信息技能。人才资源是第一资源，人才竞争是最终的竞争。要完善人才培养、选拔、使用、评价、激励机制”“全面开展国家工作人员信息化培训和考核”。

网信人才的培养受到党和国家的高度重视，网信干部不仅是网信人才的重要组成，更是推进网信事业发展的中坚力量。为了提高网信干部的业务和知识水平，加强网信干部培训工作，完善培训教材体系，中央网信办提出需要编写一系列与网络安全和信息化密切相关的培训教材，确保培训教材具备针对性、实用性、科学性、可读性，力争出精品、创特色。根据上述要求，开展了网络安全领域培训的调研工作，并组织专家编写本丛书，作为开展网信干部相关培训工作的辅导教材。

为了保证质量，对丛书做了规划，丛书的目录和大纲征求了信息安全专业教学指导委员会专家的意见，由中国网络空间安全协会秘书处负责丛书编写的组织工作，由中国网络空间研究院与中国网络空间安全协会负责编写，并以自愿申领与定向邀请相结合的方式，委托国内知名科研院所和企事业单位的专家学者参与丛书的编写和统稿工作。

衷心希望本丛书能够提高网信干部的网络安全知识水平，促进网信干部的培训工作，为推进网信人才培养和网信事业发展做出应有的贡献。

中国工程院院士 方滨兴

2016年8月23日

前　言

随着信息化的发展，政府部门、金融机构、企事业单位、商业组织等对信息系统的依赖程度日益增强，网络安全问题受到普遍关注。同时，信息系统也成了威胁、攻击以及破坏的对象。对信息在网络上的存储、传输和共享等过程的非法利用和破坏，使得如何确保信息系统的安全成为现阶段亟待解决的重要问题。

安全测评是由具有检测技术能力的权威机构，依据国家标准、行业标准、地方标准或相关技术规范，按照严格程序对信息技术产品、网络与信息系统的安全保障能力进行的科学、公正的综合测试评估活动，对测评对象的安全要求符合性和安全保障能力做出综合评价，提出相关改进建议，并出具相应的安全测评报告。

网络安全问题直接影响到国家安全，世界各国都高度重视，并纷纷通过颁布标准、实行有效的测评认证制度等方式，对信息技术产品和信息系统实行严格的管理与控制。各国政府均投入巨资，由国家主导，针对不同的网络安全需求和技术领域研发相应的测评技术、方法和工具，以建立有效的网络安全测评认证体系，为保障网络安全发挥重要作用。因此，网络安全测评的技术方法、测试工具、体系建设、制度建设等显得越来越重要，并受到各个国家的高度重视。

作为网信干部培训辅导丛书的重要教材，本书系统介绍了网络安全测评的理论、方法与应用，共 10 章，分为四大部分。第一部分（第 1 章、第 2 章），介绍信息安全测评思想和方法，涉及信息安全保障体系、安全测评作用、国内外发展情况、安全测评基本概念以及合规性与标准等内容；第二部分（第 3 章～第 5 章），介绍安全测评的主要技术和实施流程，涉及数据安全、主机安全以及网络安全等测评内容；第三部分（第 6 章～第 8 章），介绍威胁识别、脆弱性识别及风险评估等内容；第四部分（第 9 章、第 10 章），介绍具体测评案例以及国外在信息安全测评领域的最新进展，涉及安全评估工具、Web 安全测评、移动安全测评、云计算环境安全测评以及工控系统安全测评等内容。

本书由中国网络空间研究院与中国网络空间安全协会负责编写，参与调研与编写的人员

还有来自国内知名科研院所和企事业单位的专家学者。本书目录与大纲通过了信息安全专业教学指导委员会专家的咨询论证，并利用中国网络空间安全协会专家群的优势组织开展编写工作，向业界专家发出编写任务认领邀请，经遴选后委派编写工作。聘请专家对提交的稿件进行多次统稿，最终通过专家审稿会的评审。方滨兴院士对本书的整体筹划和布局给予了悉心指导，陈晓桦研究员负责本书的内容安排与组织，连一峰研究员负责本书的统稿，参与编写和组稿的还有（以下按姓氏笔画排序）王海龙、仇新梁、布宁、冯燕春、李柏松、李斌、肖新光、余慧英、邹维、赵阳、顾健、徐克付、高志民、高强裔、龚晓锐、程叶霞、霍玮、霍珊珊，在此表示感谢！

由于水平有限，编写过程中难免有错误之处，欢迎大家批评指正！

目　录

第一部分　基本思想和方法

第二部分 主要技术和实施流程

第三部分 主要方法与内容

第四部分 案例及国外最新进展

第一部分
基本思想和方法

第 1 章 安全测评概述

1.1 安全测评在网络安全保障体系中的作用

随着信息技术的迅猛发展，世界各国的信息化进程急剧加快。信息与网络空间给各国的政治、经济、文化、科技、军事和社会管理等各个方面都注入了新的活力。人们在享受信息化带来的众多好处的同时，也面临着日益突出的信息安全与保密问题。

事实上，信息安全问题一直伴随着人类社会发展。在政治、军事斗争、商业竞争和个人隐私保护等活动中，人们常常希望他人不能获知或篡改重要信息，或者需要查验所获得的信息的可信性。在网络环境中，国家秘密和商业秘密的保护，特别是政府上网后对涉密信息和敏感信息的保护，网上各种行为者的身份确认与权责利的确认，高度网络化的业务（商务、政务等）信息系统的正常运行，网络银行及电子商务中的安全支付与结算，金融机构的数据保护与管理系统的反欺诈，将成为社会各领域关注的焦点，甚至对社会稳定和国家安全带来重要影响。

信息安全测评对信息安全模块、产品或信息系统的安全性进行验证、测试、评价和定级，目的在于规范它们的安全特性。其作用在于通过验证、测试、评估信息模块/产品/系统的各种关键安全功能、性能以及运维使用情况，发现模块、产品或者系统在设计、研发、生产、集成、建设、运维、应用过程中存在的信息安全风险、发生或可能发生的信息安全问题，鉴定产品质量，监控系统行为，警示安全风险，保障网络与信息安全。

1.1.1 信息安全概述

1.1.1.1 信息安全的属性

信息安全是指保障国家、机构、个人的信息空间、信息载体和信息资源不受来自内外各种形式的危险、威胁、侵害和误导的外在状态和方式及内在主体感受。信息技术的发展也促使信息安全的内涵不断延伸，可以理解为信息系统抵御意外事件或恶意行为的能力，这些事

件和行为将会危及存储、处理或传输的数据或由这些系统所提供服务的机密性、完整性、可用性、不可否认性、真实性和可控性，这 6 个属性是信息安全的基本属性。

机密性：是指信息不被非授权解析，信息系统不被非授权使用的特性。保证数据即使被捕获也不会被解析，保证信息系统即使能够被访问也不能够越权访问与其身份不相符的信息。

完整性：是指信息不被篡改的特性。确保网络中所传播的信息不被篡改或任何被篡改了的信息都可以被发现。

可用性：是指信息与信息系统在任何情况下都能够在满足基本需求的前提下被使用的特性。这一特性存在于物理安全、运行安全层面上。确保基础信息网络与重要信息系统的正常运行能力，包括保障信息的正常传递，保证信息系统正常提供服务等。

不可否认性：是指能够保证信息系统的操作者或信息的处理者不能否认其行为或处理结果的特性。这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。

真实性：是指信息系统在交互运行中确保并确认信息的来源以及信息发布者的真实可信及不可否认的特性。保证交互双方身份的真实可信以及交互信息及其来源的真实可信。

可控性：是指在信息系统中具备对信息流的监测与控制特性。互联网上针对特定信息和信息流的主动监测、过滤、限制、阻断等控制能力。

1.1.1.2 信息安全的多角度分析

信息安全的问题既可以从客观存在的角度来看，也可以从主观意识的角度来看。从客观的角度看，所看到的是技术的层面；从主观的角度看，所看到的则是社会的层面。

信息安全从技术层面上看可以分为 4 个方面：物理安全、运行安全、数据安全和内容安全。不同的方面在客观上反映了技术系统的不同安全属性，也决定了信息安全技术不同的表现形式。

1. 物理安全

物理安全是围绕网络与信息系统的物理装备及其有关信息的安全。主要涉及信息及信息系统的电磁辐射、抗恶劣工作环境等方面的问题。面对的威胁主要有自然灾害、电磁泄露、通信干扰等。主要的保护方式有数据和系统备份、电磁屏蔽、抗干扰、容错等。

2. 运行安全

运行安全是围绕网络与信息系统的运行过程和运行状态的安全。主要涉及信息系统的正常运行与有效的访问控制等方面的问题。面对的威胁包括网络攻击、网络病毒、网络阻塞、系统安全漏洞利用等。主要的保护方式有访问控制、病毒防治、应急响应、风险分析、漏洞扫描、入侵检测、系统加固、安全审计等。

3. 数据安全

数据安全是围绕数据（信息）的生成、处理、传输、存储等环节中的安全。主要涉及数据（信息）的泄密、破坏、伪造、否认等方面的问题。面对的威胁主要包括对数据（信息）的窃取、篡改、冒充、抵赖、破译、越权访问等。主要的保护方式有加密、认证、访问控制、鉴别、签名等。

4. 内容安全

内容安全是围绕非授权信息在网络上进行传播的安全。主要涉及对传播信息的有效控

制。面对的威胁主要包括通过网络迅速传播有害信息、制造恶意舆论等。主要的保护方式有信息内容的监测、过滤等。

信息安全从社会层面的角度来看，则反映在网络空间中的舆论文化、社会行为与技术环境 3 个方面。

1. 舆论文化

互联网的高度开放性，使网络信息得以迅速而广泛地传播，且难以控制，使传统的国家舆论管制的平衡被轻易打破，进而冲击着国家安全。境内外敌对势力、民族分裂组织利用信息网络，不断散布谣言、制造混乱、推行与我国传统道德相违背的价值观。有害信息的失控会在意识形态、道德文化等方面造成严重后果，导致民族凝聚力下降和社会混乱，直接影响到国家现行制度和国家政权的稳固。

2. 社会行为

有意识地利用或针对信息及信息系统进行违法犯罪的行为，包括网络窃（泄）密、散播病毒、信息诈骗、为信息系统设置后门、攻击各种信息系统等违法犯罪行为；控制或致瘫基础信息网络和重要信息系统的网络恐怖行为；国家间的对抗行为——信息网络战。

3. 技术环境

由于信息系统自身存在的安全隐患，而难以承受所面临的网络攻击，或不能在异常状态下运行。主要包括系统自身固有的技术脆弱性和安全功能不足；构成系统的核心技术、关键装备缺乏自主可控性；对系统的宏观与微观管理的技术能力薄弱等。

1.1.1.3　信息安全的威胁

有威胁才会有安全问题，信息安全防护是针对威胁制定的对策。信息安全威胁的产生是社会发展到一定阶段的产物，其产生的根本原因是不法分子的私欲，当然还有其他直接、间接的原因。信息安全的威胁主要有以下几种。

1. 来源威胁

现在几乎所有的 CPU、操作系统、外设、网络系统甚至一些加密解密工具都来源于国外，这就相当于自己的秘密掌握在别人手里一样，不可能不受制于人。

2. 传输渠道威胁

信息要经过有线或无线的通道来进行传输。信息在传输的过程中可能被窃听、篡改、伪造。信息的安全受到威胁，合法用户的权益也受到侵害。信息的传输还要经过有形和无形的介质，由于外界环境的因素会使信号减弱、失真、丢失，因此传输的信号被严重破坏。

3. 设备故障威胁

设备的故障会导致通信中断。在整个信息系统中，硬件设备非常多，因而故障率也非常高。

4. 网络人员威胁

主要体现在 2 个方面：（1）软件开发者在开发的软件中还有残留错误，往往这些埋藏很深的错误会导致不可挽回的损失；（2）网络管理员的文化素质和人品素质影响着网络安全。网络管理员是最直接接触网络机密的人，他们有机会窃取用户的密码以及其他秘密资料，并且他们的行为可能会破坏网络的完整性，是对信息安全最直接的威胁。