

<<信息安全测评与风险评估>>

图书基本信息

书名：<<信息安全测评与风险评估>>

13位ISBN编号：9787121079924

10位ISBN编号：7121079925

出版时间：2009-1

出版时间：向宏、傅鹏、詹榜华、何德全 电子工业出版社 (2009-01出版)

作者：向宏 等著

页数：404

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<信息安全测评与风险评估>>

内容概要

《“信息化与信息社会”系列丛书·高等学校信息安全专业系列教材：信息安全测评与风险评估》分为三部分共13章。

第1部分（第1、2章）介绍信息安全测评思想和方法，是全书的灵魂；第2部分（第3章至第6章）介绍测评技术和流程；第3部分（第7章至第13章）介绍风险评估、应急响应、法律法规和信息安全管理体系。

全书涉及了信息安全等级保护、风险评估、应急响应和信息安全管理体系等相关的国家标准，均属于我国开展信息安全保障工作中所依据的核心标准集。

《“信息化与信息社会”系列丛书·高等学校信息安全专业系列教材：信息安全测评与风险评估》通过理论与实践紧密联系的方式，向读者介绍如何依据国家有关标准要求进行信息系统的安全测评和风险评估。

读者读完《“信息化与信息社会”系列丛书·高等学校信息安全专业系列教材：信息安全测评与风险评估》之后，既可掌握国家有关标准，更能在实际工作中去贯彻执行这些标准。

《“信息化与信息社会”系列丛书·高等学校信息安全专业系列教材：信息安全测评与风险评估》主要是针对全日制普通高等学校信息安全专业高年级本科生编写的，但从事信息安全测评工作的有关读者也可从中获得借鉴。

书籍目录

第1章 信息安全测评思想序幕：何危最险？

要点：本章结束之后，读者应当了解和掌握1.1 信息安全测评的科学精神1.2 信息安全测评的科学方法1.3 信息安全测评的贯标思想1.4 信息安全标准化组织1.4.1 国际标准化组织1.4.2 国外标准化组织1.4.3 国内标准化组织1.5 本章小结尾声：三位旅行者观感第2章 信息安全测评方法序幕：培根的《新工具》

要点：本章结束之后，读者应当了解和掌握2.1 为何测评2.1.1 信息系统安全等级保护标准与TCSEC2.1.2 中国的计算机安全等级保护标准2.1.3 安全域2.2 何时测评2.3 测评什么2.3.1 外网测评特点2.3.2 内网测评特点2.4 谁来测评2.5 如何准备测评2.6 怎样测评2.6.1 测评案例——“天网”工程2.6.2 启动“天网”测评2.7 本章小结尾声：比《新工具》更新的是什么？

观感第3章 数据安全测评技术序幕：谜已解，史可鉴要点：本章结束之后，读者应当了解和掌握3.1 数据安全测评的诸方面3.2 数据安全测评的实施3.2.1 数据安全访谈调研3.2.2 数据安全现场检查3.2.3 数据安全测试3.3 本章小结尾声：窃之犹在！

观感第4章 主机安全测评技术序幕：第一代黑客要点：本章结束之后，读者应当了解和掌握4.1 主机安全测评的诸方面4.2 主机安全测评的实施4.2.1 主机安全访谈调研4.2.2 主机安全现场检查4.2.3 主机安全测试4.3 本章小结尾声：可信赖的主体观感第5章 网络安全测评技术序幕：围棋的智慧要点：本章结束之后，读者应当了解和掌握5.1 网络安全测评的诸方面5.2 网络安全测评的实施5.2.1 网络安全访谈调研5.2.2 网络安全现场检查5.2.3 网络安全测试5.3 本章小结尾声：墙、门、界观感第6章 应用安全测评技术序幕：“机器会思考吗？”

要点：本章结束之后，读者应当了解和掌握6.1 应用安全测评的诸方面6.2 应用安全测评的实施6.2.1 应用安全访谈调研6.2.2 应用安全现场检查6.2.3 应用安全测试6.3 本章小结尾声：史上最“万能”的机器观感第7章 资产识别序幕：伦敦大火启示录要点：本章结束之后，读者应当了解和掌握7.1 风险概述7.2 资产识别的诸方面7.2.1 资产分类7.2.2 资产赋值7.3 资产识别案例分析7.3.1 模拟案例背景简介7.3.2 资产分类7.3.3 资产赋值7.3.4 资产识别输出报告7.4 本章小结尾声：我们究竟拥有什么？

观感第8章 威胁识别序幕：威胁在哪里？

要点：本章结束之后，读者应当了解和掌握8.1 威胁概述8.2 威胁识别的诸方面8.2.1 威胁分类——植树和剪枝8.2.2 威胁赋值——统计8.3 威胁识别案例分析8.3.1 “数字兰曦”威胁识别8.3.2 威胁识别输出报告8.4 本章小结尾声：在鹰隼盘旋的天空下观感第9章 脆弱性识别序幕：永恒的阿基里斯之踵要点：本章结束之后，读者应当了解和掌握9.1 脆弱性概述9.2 脆弱性识别的诸方面9.2.1 脆弱性发现9.2.2 脆弱性分类9.2.3 脆弱性验证9.2.4 脆弱性赋值9.3 脆弱性识别案例分析9.3.1 信息环境脆弱性识别9.3.2 公用信息载体脆弱性识别9.3.3 脆弱性仿真验证9.3.4 脆弱性识别输出报告9.4 本章小结尾声：木马歌观感第10章 风险分析序幕：烽火的演变要点：本章结束之后，读者应当了解和掌握10.1 风险分析概述10.2 风险计算10.2.1 相乘法原理10.2.2 风险值计算示例10.3 风险定级10.4 风险控制10.5 残余风险10.6 风险评估案例分析10.6.1 信息环境风险计算10.6.2 人员资产风险计算10.6.3 管理制度风险计算10.6.4 机房风险计算10.6.5 信息环境风险统计10.6.6 公用信息载体风险计算10.6.7 专用信息及信息载体的风险计算10.6.8 风险计算报告10.6.9 风险控制示例10.6.10 风险控制计划10.7 本章小结尾声：“勇敢”的反面是什么观感第11章 应急响应序幕：虚拟社会的消防队要点：本章结束之后，读者应当了解和掌握11.1 应急响应概述11.2 应急响应计划11.2.1 应急响应计划的准备11.2.2 应急响应计划制定中应注意的问题11.2.3 应急响应计划的制定11.2.4 应急响应计划的培训、演练和更新11.2.5 文档的保存、分发与维护11.3 应急响应计划案例分析11.3.1 南海大学信息安全应急响应计划示例11.3.2 “南洋烽火计划”11.4 本章小结尾声：如何变“惊慌失措”为“从容不迫”观感第12章 法律和法规序幕：神话世界中需要秩序吗要点：本章结束之后，读者应当了解和掌握12.1 计算机犯罪概述12.2 信息安全法律和法规简介12.2.1 美国有关法律12.2.2 中国信息安全法律和法规的历史沿革12.3 本章小结尾声：从囚徒困境说起观感第13章 信息安全管理体系序幕：武学的最高境界要点：本章结束之后，读者应当了解和掌握13.1 ISMS概述13.2 ISMS主要内容13.2.1 计划（Plan）13.2.2 实施（Do）13.2.3 检查（Check）13.2.4 处置（Act）13.3 本章小结尾声：实力源于何处观感参考文献

<<信息安全测评与风险评估>>

章节摘录

版权页：插图：1.1 信息安全测评的科学精神如果有读者认为信息安全测评就是从事神秘的“hacker”工作，对此我们不敢苟同。

我们认为信息安全测评首先是探索真理、发现真相的科学。

因此，与其他自然科学一样，信息安全测评也遵循着一般的客观规律。

要掌握好信息安全测评的理论、方法和技术，首先应该明确一名安全测评工程师应该具备什么样的科学精神和素养？

这是从事信息安全测评工作的前提和基础。

有了这些科学精神，再加上训练有素的工作作风和您偏爱的某种hacker气质，也许就是作者心目中的安全测评工程师了。

那么，首先要具备什么样的科学精神呢？

我们认为，“怀疑、批判、创新、求实、协作”是一名科学工作者必须具备的科学素养，同样也是指导我们进行信息系统安全测评的基本精神和思想。

这种科学精神源自于五百多年前的文艺复兴及其后来的启蒙运动（Enlightenment）。

从16世纪开始，欧洲一批批进步的宗教人士、哲学家、科学家和艺术家们前赴后继，对万能上帝存在的合理性提出质疑，对中世纪欧洲宗教法庭的权威发起挑战，终于“将科学从神学婢女的地位中解放出来。

”1919年发生在中国著名的“五四”运动，请来的“德先生、赛先生”（民主、科学），则是这场伟大的启蒙运动在古老东方的美妙回声，并持续影响着一代代中国人。

尽管这场人类历史上轰轰烈烈的思想解放运动不属于本书撰写的范畴，但请读者记住，包括信息安全学科在内的各门自然科学的发展深受其影响。

而作为一门新兴的IT学科分支，信息安全测评也必将从前辈们的思想源泉中源源不断地吸取营养。

如果读者觉得上面这些“说教”非常抽象，那么就换个角度来思考吧。

设想您作为一名信息安全测评工程师，正在对一个信息系统，如某重要金融信息系统进行安全测评。

该信息系统建设之前，已经通过了众多专家的评审。

现在您发现这个投入了巨资的建设方案并不合理。

请问您的质疑有依据吗？

您的质疑合理吗？

你能实事求是地指出问题出在什么地方吗？

您的领导和其他测评工程师支持您吗？

1.2 信息安全测评的科学方法如果说信息安全测评工作最主要的方法是系统科学，系统工程的方法，有的读者可能会感到生疏或迷茫。

那么让我们换一个角度来思考吧。

您知道Windows操作系统，如Windows2003有多少行代码吗？

5000万行！

参与开发与测试的人员接近8000人。

而这仅仅是一个大型信息系统的某一台PC终端可能安装的若干软件之一。

您知道现代超大规模集成电路（VLSI）是一个什么概念吗？

Intel公司利用纳米工艺制造的45nmPenrynWolfdale双核芯片，集成了近4亿个晶体管，核心面积仅为107rrrrri2（一个手指甲大小）！

而这仅仅是一台计算机中若干硬件的一部分。

您知道一名配备得有单兵数字化作战系统的二1：兵在作战时，身后有多少软、硬件在支撑他吗？

太空中有数百颗卫星、天空中有成千架作战飞机、地面上有成群的战车火炮、大海中有各种军舰。

而这些“武装到牙齿”的战争怪兽的指挥中枢，又是由千千万万的计算机软、硬件构成的。

他们相互交织在一起，构成了一个庞大的“人一机合一”的信息网络……我们在这里无意扮演桑鲁卓公主的角色来讲述信息时代“一千零一夜”的故事，但想象力丰富的读者应该对现代信息系统的复杂

<<信息安全测评与风险评估>>

性有了一个大概的认识了吧？

现在让我们回到本节的主题，什么是信息安全测评的科学方法？

由于我们面临的测评对象往往是一个复杂、庞大的信息系统，“杀牛就得用牛刀”，因此我们需要采用解决系统复杂性的科学方法—系统科学方法。

由于篇幅所限，这里仅仅简要介绍系统科学发展的主要脉络，有兴趣的读者可以参见诸如《系统科学》（许国志主编，上海科技教育出版社.2 000）等著作。

熟悉这部分内容的读者则可以进入下一节。

<<信息安全测评与风险评估>>

编辑推荐

《信息安全测评与风险评估》是普通高等教育“十一五”国家级规划教材，“信息化与信息社会”系列丛书之高等学校信息安全专业系列教材之一。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>