第一图书网, tushu007.com

<<信息安全等级测评师培训教程>>

图书基本信息

书名：<<信息安全等级测评师培训教程>>

13位ISBN编号：9787121118111

10位ISBN编号：7121118114

出版时间：2010-10

出版时间：电子工业

作者：公安部信息安全等级保护评估中心

页数：371

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

前言

信息安全等级保护制度是国家信息安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。
国务院法规和中央文件明确规定，要实行信息安全等级保护，重点保护基础信息安全网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度。
信息安全等级测评师等级保护工作的重要环节，信息系统备案单位通过委托测评机构开展等级测评，可以查找系统安全隐患和薄弱环节，明确系统与相应等级标准要求的差距和不足，有针对性地进行安全建设整改。
等级测评工作涉及的信息系统范围广、政策性强，需要建立专门的测评机构专业开展测评工作，需要培养一批专门从事等级测评工作的专业技术人员。
我们结合近些年的工作实践，在公安部网络安全保卫局的指导下，编写了这本教程，对开展信息安全等级测评工作的主要内容和方法进行了介绍，供读者参考、借鉴。
本教材除了适用于等级测评师培训外，还适用于信息系统运营使用单位的运维、管理人员，有助于他们在信息系统运行维护和组织本单位系统自查过程中有针对性的开展相应工作。
由于水平有限，书中难免有不足之处，敬请读者指正。

内容概要

本教材结合我国信息安全等级保护制度编写，是长期从事信息安全等级测评人员结合等级测评工作实践的总结，根据信息安全等级测评师（初级）岗位特点、能力要求进行编写，用以指导等级测评人员开展信息安全等级测评工作。
内容包括：网络安全测评，主机安全测评，应用安全测评，数据安全测评，物理安全测评，安全管理测评，工作测试等内容。
　本书为信息安全等级测评师（初级）专用教材，也可作为信息安全测评人员、信息系统运行维护人员、信息系统安全设计、建设和集成人员、大专院校信息安全相关专业人员参考用书。

书籍目录

第1章 网络安全测评 1.1 网络全局 1.1.1 结构安全 1.1.2 边界完整性检查 1.1.3 入侵防范 1.1.4 恶意代码防范 1.2 路由器 1.2.1 访问控制 1.2.2 安全审计 1.2.3 网络设备防护 1.3 交换机 1.3.1 访问控制 1.3.2 安全审计 1.3.3 网络设备防护 1.4 防火墙 1.4.1 访问控制 1.4.2 安全审计 1.4.3 网络设备防护 1.5 入侵检测／防御系统 1.5.1 访问控制 1.5.2 安全审计 1.5.3 网络设备防护 第2章 主机安全测评 2.1 操作系统测评 2.1.1 身份鉴别 2.1.2 访问控制 2.1.3 安全审计 2.1.4 剩余信息保护 2.1.5 入侵防范 2.1.6 恶意代码防范 2.1.7 资源控制 2.2 数据库系统测评 2.2.1 身份鉴别 2.2.2 访问控制 2.2.3 安全审计 2.2.4 资源控制 第3章 应用安全测评 3.1 身份鉴别 3.2 访问控制 3.3 安全审计 3.4 剩余信息保护 3.5 通信完整性 3.6 通信保密性 3.7 抗抵赖 3.8 软件容错 3.9 资源控制 第4章 数据安全测评 4.1 数据完整性 4.2 数据保密性 4.3 备份和恢复 第5章 物理安全测评 5.1 物理位置的选择 5.2 物理访问控制 5.3 防盗窃和防破坏 5.4 防雷击 5.5 防火 5.6 防水和防潮 5.7 防静电 5.8 温湿度控制 5.9 电力供应 5.10 电磁防护 第6章 安全管理测评 6.1 安全管理制度 6.1.1 管理制度 6.1.2 制定和发布 6.1.3 评审和修订 6.2 安全管理机构 6.2.1 岗位设置 6.2.2 人员配备 6.2.3 授权和审批 6.2.4 沟通和合作 6.2.5 审核和检查 6.3 人员安全管理 6.3.1 人员录用 6.3.2 人员离岗 6.3.3 人员考核 6.3.4 安全意识教育和培训 6.3.5 外部人员访问管理 6.4 系统建设管理 6.4.1 系统定级 6.4.2 安全方案设计 6.4.3 产品采购 6.4.4 自行软件开发 6.4.5 外包软件开发 6.4.6 工程实施 6.4.7 测试验收 6.4.8 系统交付 6.4.9 系统备案 6.4.10 等级测评 6.4.11 安全服务商选择 6.5 系统运维管理 6.5.1 环境管理 6.5.2 资产管理 6.5.3 介质管理 6.5.4 设备管理 6.5.5 监控管理和安全管理中心 6.5.6 网络安全管理 6.5.7 系统安全管理 6.5.8 恶意代码防范管理 6.5.9 密码管理 6.5.10 变更管理 6.5.11 备份与恢复管理 6.5.12 安全事件处置 6.5.13 应急预案管理 第7章 工具测试 7.1 测试目的 7.2 测试内容 7.3 测试流程 7.3.1 收集信息 7.3.2 规划接入点 7.3.3 编制《工具测试作业指导书》 7.3.4 现场测试 7.3.5 结果整理 7.4 注意事项 7.5 实例解析 7.5.1 系统信息 7.5.2 分析过程 7.5.3 完成作业指导书 7.6 扫描工具概述 7.7 使用方法介绍 7.7.1 准备工作 7.7.2 网络接入 7.7.3 初次配置 7.7.4 定制扫描任务 7.7.5 扫描策略和注意事项 7.7.6 报告生成 7.7.7 报表分析 附录A 信息安全技术 附录B 网络攻击技术 附录C 核查表示例 附录D 工具测试作业指导书模板 参考文献

章节摘录

插图：1.1.2边界完整性检查a）应能够对非授权设备私自联到内部网络的行为进行检查，准确定位，并对其进行有效阻断。
【描述】可以采用技术手段和管理措施对“非法接入”行为进行检查。
技术手段包括网络接入控制、关闭网络设备未使用的端口、IP／MAC地址绑定等。
管理措施包括进入机房全程陪同、红外视频监控等。
【检查方法】访谈网络管理员，询问采用何种技术手段或管理措施对非授权设备私自联到内部网络的行为进行检查、定位和阻断。
如果采用技术手段则询问采用了何种技术手段，并在网络管理员的配合下验证其有效性。
同时要询问相关的管理措施。
b）应能够对内部网络用户私自联到外部网络的行为进行检查，准确定位，并对其进行有效阻断。
【描述】主要用来发现和管理用户非法建立通路连接非授权网络的行为，非法外联行为绕过了边界安全设备的统一管理，打破了网络边界的统一控制管理，使得内网面临的安全风险增大。
可以依靠内网安全管理系统的非法外联监控功能或者非法外联软件实现，通过非法外联监控的管理，可以防止用户访问非信任网络资源，并防止由于访问非信任网络资源而引入安全风险或者导致信息泄密。

编辑推荐

《信息安全等级测评师培训教程(初级)》：“十一五”国家重点图书出版规划项目信息安全等级保护测评工作是信息安全等级保护工作的重要环节，是专门机构针对信息系统开展的一种专业性、服务性的检测活动。
等级测评工作涉及的信息系统范围广、敏感性强，参与的测评机构及测评人员复杂，如果缺乏对测评机构和测评人员的管理，则难以保证等级测评的客观、公正和安全，甚至会给重要信息系统安全造成新的风险和隐患，危害国家安全和社会稳定。
为加强对测评机构及测评人员管理，稳步推进等级测评机构建设，规范等级测评活动，提高测评机构、人员的技术能力和水平，在国家信息安全等级保护协调小组的领导下，全国组织开展信息安全等级保护等级测评体系建设工作，以保障等级保护工作的顺利开展。

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