<<信息安全管理基础>>

图书基本信息

书名：<<信息安全管理基础>>

13位ISBN编号：9787115176349

10位ISBN编号：7115176345

出版时间：2008-5

出版时间：人民邮电出版社

作者：北京大学电子政务研究院电子政务与信息安全技术实验室

页数：305

<<信息安全管理基础>>

内容概要

为了推进我国信息化人才建设，CEAC国家信息化培训认证管理办公室组织IT和培训领域的资深专家精心编写了国家信息化计算机教育认证系列教材。
本书作为国家信息化计算机教育认证项目电子政务与信息安全培训认证专项的教材之一，以国际主流的安全技术为基础，详细介绍了信息安全涉及的安全理论知识与技术。
本书根据企事业单位和信息安全从业人员的实际需求，深入浅出地介绍了信息安全的物理安全、身份鉴别与认证、风险管理、安全管理策略等内容，并详细阐述了用户必须了解的安全法规和标准。
本书结构清晰，讲解详细，并在每章后配有丰富的思考与练习题。
非常适合作为信息安全技术的标准培训教程，也可作为大中专院校、高职高专相应课程的教材和辅导教材，还可供读者自学使用。

<<信息安全管理基础>>

书籍目录

章节摘录

第1章　信息安全管理概述随着信息技术的发展，人们在享受信息技术带来的方便与高效的同时也面临着严重的信息安全的威胁。
怎样保证信息被合法有效的利用，是目前信息安全技术所面临的一大课题。
构建良好的信息安全管理策略是构建信息安全平台的前提条件。
1.1　全球信息安全发展形势Intemet是信息传输的集中地，在上面充斥着大量有用和无用的信息。
Internet是一个庞杂的系统，其设计本身不可避免会出现很多不安全的因素。
Intemet是一个开放式的网络，任何使用者都可能成为它的安全威胁者。
1.1.1 互联网骨干网络面临的安全威胁Intemet主要由路由器和DNS服务器两大基本架构组成，其中路由器构成Internet的主干，DNS服务器负责将域名解析为IP地址。
攻击互联网骨干网络最直接的方式就是攻击互联网主干路由器和DNS服务器。
如果一个攻击者能成功地破坏主干路由器用来共享路由信息的边界网关协议（BGP），或者更改网络中的DNS服务器，就会使Intemet陷入一片混乱。
为了寻找一些能够使主干路由器和DNS服务器彻底崩溃或者能够取得其系统管理权限的缓冲溢出或其他安全漏洞，恶意的高级攻击者通常会非常仔细地检查一些主干路由器和DNS服务器的服务程序代码和它们之间的通信协议的实现代码。
路由代码非常复杂，目前已经发现并已修复了许多重要的安全问题，但是仍旧可能存在许多更严重的问题，并且很可能被黑客发现和利用。
DNS软件过去经常发生缓冲溢出这样的问题，在以后也肯定会发生类似的问题。
如果攻击者发现了路由、DNS或通信协议的安全漏洞，并对其进行大举攻击，那么大部分Intemet将会迅速瘫痪。
2002年8月，互联网赖以运行的基础通信规则之一——ASN NO.1信令的安全脆弱性就严重威胁了互联网骨干网基础设施的安全。
黑客利用ASN NO.1信令的安全漏洞开发相应的攻击程序，关闭ISP的骨干路由器、交换机和众多的基础网络设备，可最终引起整个互联网瘫痪。
ASN NO.1信令的安全脆弱性使得超过100家的计算机网络设备提供商将要为此付出代价，而弥补这些缺陷的投入将超过1亿美元。
由于多个互联网通信协议都是基于ASN NO.1计算机网络语言的，因此ASN NO.1的脆弱性将广泛威胁通信行业。
最为显著的例子就是造成SNMP协议多个安全漏洞。

<<信息安全管理基础>>

编辑推荐

《国家信息化计算机教育认证CEAC指定教材·信息安全管理基础》结构清晰，讲解详细，并在每章后配有丰富的思考与练习题。
非常适合作为信息安全技术的标准培训教程，也可作为大中专院校、高职高专相应课程的教材和辅导教材，还可供读者自学使用。

<<信息安全管理基础>>

版权说明