中国通信企业协会网络安全人员能力认证考试知识点大纲

管理类基础级(CACE-CPAC-BLM)

中国通信企业协会网络安全人员能力认证中心
2017 年 3 月

目录

第一部分综述

第1章 网络安全基础知识

1.1 网络安全概述

1) 了解网络安全的概念
2) 了解网络安全的 5 个特性
3) 了解不同的人员对网络安全的看法
4) 掌握网络安全的重要性

1.2 网络安全问题产生原因

1.2.1人为的失误

1) 了解人为的失误原因
2) 了解人为的失误危害
3) 掌握人为的失误的分类与各自的特点

1.2.2有目的的驱使

了解有目的驱使者的类别和特点

1.2.3计算机系统的脆弱性

1) 了解网络系统的脆弱性的基本概念
2) 掌握网络系统的脆弱性表现的 7 个方面

1.2.4计算机病毒

1) 了解计算机病毒的概念、特点

2) 了解计算机病毒的生命周期

3) 了解计算机病毒的传播的方式

4) 了解计算机病毒的具体划分

1.2.5黑客技术的普及

1) 了解黑客技术普及的原因

2) 了解黑客技术和网络安全的关系

3) 了解黑客技术对网络安全的影响

1.3 常见安全事件分类

1.3.1有害程序事件

1) 了解有害程序事件的概念

2) 掌握有害程序事件的 7 个主要事件类型

3) 了解每个事件类型下的具体事件内容和原理

1.3.2网络攻击事件

1) 了解网络攻击事件概念

2) 掌握网络攻击事件的 7 个主要事件类型

3) 了解每个事件类型下具体事件的概念和攻击原理

1.3.3信息破坏事件

1) 了解信息破坏事件概念

2) 掌握信息破坏事件的 6 个主要事件类型

3) 了解每个事件类型下具体事件的概念和攻击原理

1.3.4设备设施故障

1) 了解设备设施故障概念

2) 掌握设备设施故障的 4 个主要事件类型

3) 了解每个事件类型下具体事件的概念和攻击原理

1.3.5信息内容安全事件

1) 了解设备设施故障概念

2) 掌握设备设施故障的 4 个主要事件类型

3) 了解每个事件类型下具体事件的概念和攻击原理

1.3.6灾害性事件

1) 了解灾害性事件概念

2) 了解灾害性事件包括的内容

1.3.7其他事件

了解其他事件的概念

第2章 政策法规与道德规范

2.1 国家网络安全相关法律法规

了解国家安全委员会和中央网络安全和信息化领导小组，重点领会总书记“419”讲话内容和精神。

2.1.1我国网络安全管理体制

了解我国各级网络安全管理部门之间的关系和各自职责。

2.1.2网络安全相关法律法规

了解“国家网络空间主权”提法的出处，了解维护网络和信息安全的核心任务。了解《网络安全法》基本内容。了解《电信条例》基本内容。

2.1.3信息安全等级保护相关法规政策

了解《关于信息安全等级保护工作的实施意见》和《信息安全等级保护管理办法》的基本内容和要求。

2.2 电信和互联网行业网络安全管理政策

2.2.1通信网络安全相关法规政策

了解《通信网络安全防护办法》的基本内容和要求；了解《电信和互联网用户个人信息保护规定》基本内容和要求；了解《关于加强电信和互联网行业网络安全工作的指导意见》的八项工作任务。

2.2.2网络安全防护

了解安全防护的原则、方针和理念；了解定级备案的要求，了解符合性评测和风险评估的要求。了解网络安全防护监督检查工作内容。

2.2.3网络安全威胁治理

了解网络安全威胁治理相关的技术手段建设和管理情况。

2.2.4网络安全应急保障

了解《公共互联网网络安全应急预案》基本内容，了解预警分级、监测上报、应急响应的基本流程和要求。

2.3 道德规范

主要了解网络安全从业人员应当遵守的相关道德规范。相关道德规范具体可以分为通行道德规范和职业道德规范，无论通行道德规范和职业道德规范，网络安全从业人员都应遵守，道德规范是对网络安全从业人员的基本要求。

第二部分安全体系框架

第3章 国际安全标准体系概述

3.1 国际网络安全标准化组织

1) 了解国际上主要的几个网络安全标准化组织

2) 了解各组织的全程及简称

3.2 标准体系

3.2.1NIST SP 800 系列技术标准

1. SP 800-26 安全自评估指南

1) 了解标准的目的和内容

2) 了解调查表的目的

3) 了解调查表的问题的主要控制域以及五个有效的级别

4) 了解调查表的后续使用，调查表的三个主要用途

2. SP 800-30 风险管理指引

1) 掌握风险管理的主要流程以及每部分的理解

2) 了解 Sp 800-30 风险管理过程中的基本步骤以及具体涉及的内容

3) 了解 Sp 800-39 提出的三层风险管理框架

4) 了解 sp800-30 提出的风险评估过程的基本步骤及每个步骤的相关任务

3. SP 800-53 推荐安全控制措施

1) 了解 SP800-53 的主要内容

2) 了解 SP800-53 与相关其他标准间的关系

3) 了解 SP800-53 何将安全控制措施的选择应用于组织的信息系统，了解涉及到的四个步骤

4) 了解技术、管理、运行三个类中的 18 个族简的主要内容

4. SP 800-55 信息安全度量指南

1) 了解 SP 800-55 标准的目的

2) 理解信息安全度量项目应该包括 4 个相互关联的因素

3) 了解信息安全度量项目执行过程

5. SP 800-64 信息系统开发生命周期中的安全管理

1) 了解 SP 800-64 标准的目的

2) 理解 SDLC 的五个阶段

3.2.2ISO/IEC 15408

1) 了解 ISO/IEC 15408 标准的主要目的以及使用场景

2) 了解 CC 标准的安全功能要求

3) 熟悉 cc 标准的主要控制项

3.3 ISO27000 系列安全管理体系

3.3.1标准综述

1) 了解 ISO 27000 系列重要标准的编号及名称

2) 了解 ISO 27000 系列各标准之间的关系

3.3.2重点标准简介

1. ISO/IEC 27001 体系要求

1) 了解该标准的演变过程

2) 了解该标准正文部分的内容构成

3) 理解附录中个控制域的主要内容

4) 了解该标准的用途

2. ISO/IEC 27002 实用规则

1) 了解该标准与 ISO/IEC 27001 的关系

2) 掌握该标准的适用范围

3) 了解该标准的结构

3. ISO/IEC 27003 实施指南

1) 掌握该标准的用途

2) 了解该标准的结构

3) 了解 ISMS 的实施总图

4. ISO/IEC 27004 信息安全管理测量

1) 掌握该标准的用途

2) 了解该标准的核心内容

3) 了解该标准的应用场景和适用范围

5. ISO/IEC 27005 风险管理

1) 掌握该标准的用途

2) 理解信息安全风险管理的六个过程

3) 了解该标准的应用场景和适用范围

6. ISO/IEC 27006 认证机构认可要求

1) 了解该标准的主旨及框架

2) 了解该标准的适用范围

7. ISO/IEC 27011 电信行业信息安全管理指南

1) 了解该标准制定的目的和意义

2) 了解该标准的应用场景和适用范围

8. ISO/IEC 27031 信息通信技术的业务连续性管理指南

1) 了解该标准制定的目的

2) 了解该标准的核心内容

3) 了解该标准的应用场景和适用范围

9. ISO/IEC 27034 应用安全指南

1) 了解该标准制定的目的

2) 熟悉该标准中的四个核心要素

3) 了解该标准的应用场景和适用范围

10. ISO/IEC 27035 信息安全事件管理

1) 了解该标准的目的

2) 了解该标准的应用场景和适用范围

3.3.3ISMS 建设与实施

1. 现状调研
   1) 了解管理调研的几种方式
   2) 了解安全技术措施调研的几种方式
   3) 了解渗透测试的概念
2. 风险评估
   1) 掌握风险评估的几个阶段
   2) 了解每个阶段的工作内容
3. 体系文档编制
   1) 了解信息安全管理体系的文档组成
   2) 了解每一级的文件所包含的内容
   3) 体系试运行
   4) 了解体系试运行的几个环节
   5) 了解知识传递的几种方式

3.3.4ISMS 认证与审核

1) 了解 ISMS 内审的过程和方法
2) 了解内审工具
3) 了解认证的准备
4) 了解认证的实施过程

第4章 国内安全标准体系概述

4.1 国内网络安全标准化组织

1) 了解国内主要网络安全标准化组织的简称
2) 了解国内主要网络安全标准化组织的工作内容

4.2 通信网络安全防护标准

4.2.1电信网和互联网安全防护管理指南

1) 了解该标准的适用范围
2) 理解电信网和互联网安全防护体系的构成
3) 了解安全等级保护实施的基本过程
4) 了解安全风险评估实施的基本过程
5) 了解灾难备份及恢复实施的基本过程
6) 理解电信网和互联网安全防护体系中的安全等级保护、安全风险评估、灾难备份及恢复三者之间的关系

4.2.2电信网和互联网安全风险评估实施指南

1) 了解标准的主要内容和目的
2) 了解对于电信网和互联网相关系统生命周期中的风险要素
3) 熟悉风险实施的流程

4.2.3电信网和互联网灾难备份及恢复实施指南

1) 理解该标准的目的和主要的内容。
2) 了解灾难备份及恢复定级的 5 个等级的主要内容。
3) 了解不同级别对应有的技术和管理支持的要求

4.2.4电信网和互联网安全等级保护实施指南

1) 了解实施指南的主要内容与结构
2) 熟悉实施指南的安全等级保护对象
3) 熟悉安全等级保护实施的基本过程
4) 熟悉电信网和互联网及相关系统定级方法

第5章 安全体系最佳实践

5.1 安全体系设计基本方法

5.1.1行业内广泛使用的体系模型

1) 了解 IATF 纵深防御理论的主要内容及组成
2) 了解 ITU-X.805 的主要内容及核心组成
3) 了解 ISO 7498-2 的主要内容及核心思想
4) 了解 COBIT 的主要内容、核心思想及内容组成

5.2 安全体系架构

5.2.1明确保护对象、安全需求、安全策略

1) 掌握安全体系设计的原则
2) 了解保护对象的范围
3) 了解资产的分类、分级方法
4) 了解落实安全需求的原则
5) 掌握信息安全建设需求分析的主要任务
6) 掌握完整的信息安全策略及保障体系的组成及每部分的主要内容

5.2.2业务、组织、流程与标准间的映射

1) 了解流程设计的基本内容
2) 了解如何将业务、流程、组织等与适宜的标准做映射

5.2.3合理借鉴引用并本地化体系模型

1) 了解合理借鉴引用并本地化体系模型的方式

5.3 安全管理流程

1) 了解完备的网络安全工作总体工作内容
2) 了解检查维度及周期性要求
3) 了解常见检查工具
4) 了解闭环管理意义

第三部分安全运行与管理

第6章 风险评估

6.1 风险评估概述

6.1.1风险的定义

1. 风险的定义
   1) 了解国际标准中对风险的定义
   2) 理解什么是风险，即风险的组成
2. 风险与信息安全
   1) 了解风险与信息安全的关系
   2) 了解风险在信息安全中的重要性

6.1.2风险的要素

1. 风险的要素

   理解风险的要素，资产、威胁、脆弱性、控制措施的含义
2. 风险要素之间的关系
   1) 了解业务战略、资产价值、安全事件、残余风险等基本概念
   2) 理解风险的基本要素与业务战略、资产价值、安全事件、残余风险等因素的关系

6.1.3风险评估

1) 了解风险评估的概念
2) 了解风险评估在信息安全保障体系中的作用

6.2 风险评估对网络安全的重要性

6.2.1风险评估的重要性

1. 风险管理与信息安全管理
    1) 了解为什么进行信息安全风险管理
    2) 理解信息安全管理的核心内容就是风险管理
2. 风险管理的作用

    了解风险管理的作用

6.2.2建立以风险管理为基础的安全管理

1. 风险管理作为安全管理的基础
    1) 了解风险评估是信息安全工作的起点
    2) 了解信息安全就是所承担的安全风险与安全建设管理代价之间的动态平衡
2. 风险评估成功的因素

    了解风险评估成功的因素

第7章 安全运维

7.1 安全运维概述

7.1.1安全运维的定义

1) 了解安全运维的概念、含义
2) 了解企事业有安全运维需求的原因

7.1.2安全运维的现状

1) 了解安全运维的现状
2) 了解当前企事业安全运维的侧重点与不足点

7.1.3安全运维的分类

1) 掌握安全运维的分类
2) 了解其含义
3) 掌握安全运维不同方面的具体内容

7.2 安全运维方式

7.2.1安全基线

1) 了解安全基线的概念
2) 了解一些通用性基线要素的配置管理方法
3) 了解安全基线国家标准

7.2.2安全加固

1) 了解安全加固的项目实施流程
2) 掌握安全加固实施过程中关键点的处理方法

7.2.3安全监控

1) 了解安全监控的概念、检查项目以及组成部分
2) 掌握安全监控监控的主要对象和内容

7.2.4安全审计

1) 了解安全审计的概念、内容以及功能
2) 理解安全审计设计的四大要素
3) 掌握安全审计的主要内容

7.2.5应急响应

1) 了解应急响应的概念、方法、流程

2) 了解应急响应的的三个阶段

3) 掌握应急响应的方法和处理过程

7.2.6安全评估

1) 了解安全评估的概念和目标

2) 了解安全评估的主要对象和内容

7.2.7维护作业

1) 了解维护作业的概念

2) 掌握维护作业主要包含的内容

7.3 安全运维技术实现

7.3.1网络设备

1) 了解网络设备日常维护的注意事项

2) 掌握网络设备维护所包括的主要内容

7.3.2安全设备

1) 了解安全设备日常维护的注意事项

2) 掌握安全设备检查的项目和内容

7.3.3其他网关

1) 了解安全网关两种网络接入模式

2) 了解安全网关运用场景

第8章 网络安全应急响应

8.1 应急响应概述

1) 了解应急响应的简述以及和突发事件的区别

2) 了解应急响应的目标

8.2 安全事件监测方式

理解常见日志类型的记录范围及启用方式

8.2.1日志分析

理解常见日志类型的记录范围及启用方式

8.2.2后门检测

1. Windows 后门检测
    1) 了解 Windows 常规检测
    2) 理解 Windows 恶意代码检测
2. UNIX/Linux 后门检测
    1) 了解 UNIX/Linux 常规检测
    2) 理解 UNIX/Linux 系统日志
3. Webshell 检测
    1) 理解 Webshell 介绍
    2) 理解一句话木马之“小马”
    3) 理解 Webshell 查杀
    4) 理解检查文件属性的意义和方法
    5) 理解检查日志检查的意义和方法
    6) 理解工具扫描

8.2.3样本分析

1. 静态分析
    1) 理解静态分析概述
    2) 理解反病毒引擎扫描
    3) 了解哈希值（恶意样本的指纹）
    4) 了解加壳与混淆恶意代码
2. 动态分析
    1) 理解动态分析概述
    2) 了解利用沙箱分析样本行为

8.2.4流量分析

1. 网络数据包抓取与分析原理
    1) 理解 Sniffer 的分类
    2) 理解网络监听的目的
2. 工具的介绍
    1) 理解抓包工具有哪些
    2) 理解分析工具的作用和常见工具
3. 处理异常流量的方法

    理解切断连接、过滤、静态空路由过滤、异常流量限定

8.3 应急响应预案

1) 理解应急响应的简述和目的
2) 理解应急响应的生命周期
3) 理解应急响应组织分类

8.4 应急响应流程

8.4.1准备阶段

理解准备阶段的作用和此阶段的工作内容

8.4.2检测阶段

理解检测阶段的作用和此阶段的工作内容

8.4.3分类阶段

理解分类阶段的作用和此阶段的工作内容

8.4.4抑制阶段

理解抑制阶段的作用和此阶段的工作内容

8.4.5根除阶段

理解根除阶段的作用和此阶段的工作内容

8.4.6恢复阶段

理解根除阶段的作用和此阶段的工作内容

8.4.7后续阶段

理解后续阶段的作用和此阶段的工作内容

8.5 各类事件的检测分析和处置方法

8.5.1恶意代码型

1) 理解恶意代码的分类和介绍以及蠕虫和普通病毒的区别
2) 理解蠕虫的检测条件
3) 理解蠕虫的告警举例
4) 了解蠕虫的特征和应急办法

8.5.2DDOS 型

1) 理解 DDOS 攻击技术概述
2) 理解 DDOS 的分类以及各个种类的特点
3) 理解常见反射放大型攻击原理与检测

8.5.3DOS 型

1) 理解 Dos 漏洞描述
2) 了解 IP 欺骗性攻击
3) 了解 Ping 洪流攻击
4) 了解 teardrop 攻击
5) 了解 Land 攻击
6) 了解 Smurf 攻击
7) 了解 Fraggle 攻击

8.5.4 管理漏洞型

1) 理解网络管理系统简介
2) 了解网络管理系统对信息安全意义
3) 了解常见管理型漏洞

第9章 新型行业应用篇

9.1 互联网金融行业网络及信息安全管理

9.1.1互联网金融系统概述

1) 了解互联网行业监管要求及政策
2) 了解常见互联网金融系统框架
3) 了解定制购买第三方互联网金融平台及服务注意事项
4) 了解购买开源互联网金融平台二次开发注意事项
5) 了解完全自主开发平台相关事项
6) 了解互联网金融平台特点

9.1.2互联网金融系统的安全风险概述

1) 了解互联网金融网络信息系统的主要安全风险
2) 了解操作系统及运行环境的安全风险
3) 了解业务系统的安全风险
4) 了解电脑及移动客户端的安全风险
5) 了解网络的安全风险
6) 了解互联网金融信息安全管理的安全风险
7) 了解互联网金融网络信息安全风险的防范措施

9.1.3互联网金融系统安全运维

1) 了解互联网金融系统安全运维的基本原则
2) 了解互联网金融系统安全运维基础措施
3) 了解如何进行资产管理
4) 了解如何进行介质管理
5) 了解如何进行环境管理
6) 了解如何进行网络管理

7) 了解如何进行数据备份

8) 了解如何进行恶意代码防范

9) 了解如何制订互联网金融系统日常维护报告

9.1.4互联网金融系统应急响应

1) 了解应急响应的政策背景

2) 掌握应急响应的相关准备工作

3) 掌握应急响应的流程

4) 了解事件通报机制

5) 了解如何进行事件分类与定级

6) 了解应急启动相关事项

7) 了解如何进行应急处置

8) 掌握业务的恢复操作

9) 了解应急响应的后期处置

10) 了解应急响应后的总结工作

11) 了解如何计算机取证

9.1.5互联网金融企业的网络及信息安全管理制度

1) 了解安全人员管理相关事项，人员组织架构、部门职责、岗位设置

2) 了解如何进行权限分配管理

3) 了解如何规范员工的日常网络行为

4) 了解如何进行开发外包的管理，包括制度的建立、角色管理、外包行为规范、日志审查等

5) 了解如何进行安全意识管理，信息安全意识教育的基本要求，安全基本常识

第四部分安全技术

第10章 网络攻击

10.1 信息收集技术

10.1.1 信息收集作用

1) 了解黑客攻击的典型过程
2) 了解信息收集在攻击中的作用

10.1.2 域名信息收集

1) 了解域名系统的基本组成
2) 了解域名收集的作用
3) 了解域名收集的方法

10.1.3 端口扫描技术

1) 了解端口扫描的作用
2) 了解端口扫描的分类
3) 了解端口扫描的原理
4) 了解端口扫描工具

10.1.4 主机扫描技术

1) 了解主机扫描的目的
2) 了解主机扫描的工具

10.1.5 漏洞扫描技术

1) 了解漏洞扫描的目的
2) 了解漏洞扫描的目标
3) 了解漏洞扫描的工具

10.1.6 信息收集的防范

1) 了解信息收集防范的原则
2) 了解安全培训对信息收集防范的重要性
3) 了解常见的信息收集防范的方法

10.2 口令破解技术

1. 口令破解技术
    1) 了解口令破解的重要性
    2) 理解口令破解的原理，字典攻击、暴力破解、默认口令攻击的原理
2. 口令破解防范
    1) 了解什么是弱口令
    2) 了解如何设置强口令
    3) 理解口令破解的防范方法

10.3 恶意代码技术

10.3.1 恶意代码的产生

1) 了解恶意代码的定义
2) 了解恶意代码的发展历史

10.3.2 恶意代码的分类

1) 了解恶意代码的分类

2) 了解蠕虫和木马的区别

10.3.3 恶意代码传播方式

1) 了解恶意代码的传播方式
2) 了解每种传播方式的具体过程

10.3.4 恶意代码实现技术

1) 了解病毒的概念
2) 了解病毒的传播途径
3) 了解病毒的分类
4) 了解蠕虫的分类
5) 了解木马实现的原理
6) 了解僵尸网络的原理

10.4 网络攻击技术

10.4.1 欺骗技术

1) 了解什么是欺骗攻击
2) 了解 IP 欺骗攻击的原理
3) 理解 IP 欺骗的防范措施
4) 了解 ARP 欺骗攻击的原理
5) 理解 ARP 欺骗的防范措施
6) 了解 DNS 欺骗攻击的原理
7) 理解 DNS 欺骗的防范措施

10.4.2 拒绝服务攻击

1) 了解拒绝服务攻击的概念
2) 了解拒绝服务攻击的分类

3) 了解 SYNFlood 攻击原理

4) 了解 UDPFlood 攻击原理

5) 了解 Teardrop 攻击的原理

6) 了解分布式拒绝服务攻击的原理

7) 理解拒绝服务攻击的防范措施

10.4.3 后门设置与防范

1) 了解什么是后门

2) 理解后门的防范措施

10.4.4 清除痕迹与防范

1) 了解记录攻击的日志

2) 了解清楚痕迹的方法

10.5 Web 攻防技术

10.5.1 SQL 注入攻击

1) 了解常见的 Web 威胁

2) 了解 SQL 注入攻击的原理

3) 了解 SQL 注入攻击的危害

4) 理解 SQL 注入的防范措施

10.5.2 XSS 跨站脚本攻击

1) 了解跨站脚本攻击的原理

2) 了解跨站脚本攻击的危害

3) 理解跨站脚本的防范措施

10.6 社会工程学

10.6.1 社会工程学概述

1) 了解什么是社会工程学
2) 了解社会工程学的危害
3) 了解社会工程学常用的手段

10.6.2 社会工程学防范措施

理解社会工程学的防范措施

第11章 防护技术

11.1 Windows 安全防护技术

11.1.1 Windows Server 2008 简介

1) 了解 Windows 操作系统服务器版本
2) 了解 Windowsserver2008 系统的功能

11.1.2 Windows Server 2008 新特性

1) 了解 windowsserver2008 系统的新特性
2) 了解 IIS7.0
3) 理解 windowsserver2008 系统的服务器管理器

11.1.3 Windows Server 2008 版本

了解 windowsserver2008 的版本

11.1.4 Windows Server 2008 体系结构

1) 了解 windowsNT 内核的体系结构
2) 了解系统的关键进程和文件

11.1.5 Windows Server 2008 的安全性

1) 了解安全操作系统的标准
2) 了解 windowsserver2008 的安全标识符
3) 了解 windowsserver2008 的 ACL
4) 了解 windowsserver2008 的策略配置
5) 了解 windowsserver2008 的启动过程

11.2 UNIX 安全防护技术

11.2.1 Unix 系统发展历史

1) 了解 Unix 系统的发展
2) 了解 Unix 系统的常见版本
3) 了解 Unix 系统与 Linux 系统的关系

11.2.2 Unix 系统简介

1) 了解 Unix 系统的特点
2) 了解 Unix 系统的流派
3) 了解 Unix 系统的结构
4) 了解 Unix 系统的文件结构
5) 理解 Unix 系统的安全模型

11.2.3 Unix 启动和运行级别

1) 了解 Unix 系统的启动过程

2) 理解 Unix 系统的运行级别

3) 了解 Unix 系统运行级别的更改方法

11.2.4 Linux 启动和运行级别

1) 了解 Linux 启动的详细过程

2) 理解 Linux 系统的运行级别

11.3 网络安全防护技术

11.3.1 网络协议安全

1) 了解 OSI 七层模型

2) 理解 OSI 安全体系结构

3) 理解 TCP/IP 模型

4) 理解 TCP/IP 每层的主要协议

5) 理解 TCP/IP 每层的安全协议

6) 了解 IPv6 协议

7) 了解无线局域网技术

8) 了解无线局域网的认证

9) 理解 WAPI 协议

10) 了解移动通信网络的安全

11.3.2 网络安全设备

1) 理解网络设备的物理安全

2) 理解网络设备的访问控制措施

11.3.3 网络架构安全

了解网络架构安全

11.4 数据库安全防护技术

11.4.1 数据库系统概述

1) 了解数据库的概念
2) 了解数据系统的组成

11.4.2 数据库安全

1) 了解数据库安全的特性
2) 了解数据库安全的基本要求
3) 了解数据库的安全功能
4) 理解数据库的认证与访问控制
5) 了解数据库的加密
6) 理解数据库的安全审计功能
7) 理解数据库的备份与恢复
8) 理解数据库的完整性

11.4.3 数据库运行安全防护

1) 了解数据库安全防护过程
2) 了解事前安全防护内容
3) 了解事中安全防护内容
4) 了解事后安全防护内容

11.5 恶意代码防御技术

11.5.1 恶意代码的防御技术

1) 了解恶意代码的防御技术
2) 理解安全策略与意识对恶意代码的防御
3) 理解补丁管理和系统加固方法

4) 了解常见的防御恶意代码的安全设备

11.5.2 恶意代码检测技术

1) 了解恶意代码检测的分类，静态与动态方法

2) 了解恶意代码检测的原理

1) 了解特征码扫描技术

2) 了解沙箱技术

3) 了解行为检测技术

11.5.3 恶意代码清除技术

1) 了解不同的恶意代码清除

2) 了解感染引导区型恶意代码的清除

3) 了解文件感染型恶意代码的清除

4) 了解独立型恶意代码的清除

5) 了解嵌入型恶意代码的清除