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

管理类专业级(CACE-CPAC-PLM)

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 网络安全形势

1.1 全球网络空间发展情况及面临的挑战

1.1.1网络空间体系形势

1) 了解当前网络安全的重要性

2) 了解从网络空间主权、军事、斗争对手、意识形态、空间维稳等方面介绍日益紧张的趋势

1.1.2事件分析

1) 棱镜计划的事件起因、事件发展、事件影响等

2) 掌握棱镜计划事件对国家安全造成的危害

3) 掌握星风监视计划的缘由、简介和发展历史，以及四大计划的内容、危害性

4) 了解希拉里邮件门事件的事件经过

1.1.3网络空间的安全挑战

1) 了解网络空间的严峻形势

2) 掌握大规模的分布式拒绝服务攻击、众多主机和服务器受控制、翻墙软件挑战信息监控、交换机和路由器受控等安全挑战的详细内容

1.2 我国在全球网络网络空间面临的安全威胁及隐患

1.2.1我国网络空间的发展情况

1) 了解我国网络空间的的严峻形势

2) 了解中国对网络的依赖

3) 了解美国在互联网技术方面的绝对优势，进一步了解形势的严峻性

4) 了解西方国家掌握网络舆论权对于中国网络安全形势严峻性的威胁

1.2.2国家面临的威胁

1) 了解国家面临的主要威胁

2) 掌握对于每个威胁下面相应的具体案例事件和事情经过

1.2.3我国遭受网络攻击的总体趋势

1) 掌握我国遭受网络攻击的总体趋势

2) 掌握集团化、产业化的趋势、“黑客”逐渐变成犯罪职业、恶意软件的转型、网页挂马危害继续延续、利用应用软件漏洞的攻击将更为迅猛、Web2.0 的产品将受到挑战等趋势内容

1.2.4攻击案例分析

1) 中国电信全国大规模的网络故障：了解事件中会详细事件起因、主要的影响

2) 大规模 DNS 故障：了解事件中会详细事件起因、主要的影响

3) 12306 用户数据泄露：了解事件中会详细事件起因、主要的影响

4) 后门事件：了解事件中会详细事件起因、主要的影响

1.3 我国应对网络安全形势的战略规划

了解我国应对网络安全形势的战略规划

1.4 新技术的发展

1.4.1移动互联网

1) 了解从广义和狭义方面定义移动互联网概念

2) 掌握移动互联网的基本结构

3) 了解移动互联网的主要特征

4) 掌握其 Mashup 技术等关键技术

1.4.2云计算

1) 了解云计算的概念、特点

2) 了解云安全

3) 掌握云安全的应用

1.4.3大数据

1) 了解大数据的概念、结构分析等基础知识

2) 熟悉几个比较有代表性的应用案例，并学会进行分析

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 安全标准体系解析

3.1 国外安全标准简介

了解我国发布关于信息安全的标准名称

3.2 信息安全管理标准的演进历程

了解国外信息安全管理标准的演进历程

3.3 信息安全标准对比

了解各项安全标准的差异性

3.4 国内安全标准简介

了解我国发布关于信息安全的标准名称

3.5 国内外安全管理标准对比

1) 了解国内外安全标准的差异
2) 了解国内外安全标准的共性

第4章 安全体系设计方法

4.1 体系设计遵循的基本原则

1) 了解安全体系设计的基本原则
2) 了解安全体系设计的指导思想

4.2 理解安全流程各要素之间的关系

1) 了解安全体系设计遵循五个相关国内国际标准
2) 了解安全体系设计的四大保障目标
3) 了解安全体系设计的三道防线

第5章 安全体系设计实践

5.1 体系设计过程介绍

5.1.1方法与流程简述

掌握案例中整个体系设计的过程

5.1.2确定信息安全管理体系建设具体目标

5.1.3确定适合的信息安全体系方法论

5.1.4充分的现状调研和差距分析

1) 了解案例中遵循的原则
2) 掌握调研工作内容

5.1.5构建信息安全管理体系

掌握信息安全管理体系的内容

5.1.6构建信息安全技术体系

掌握信息安全技术体系的内容

5.1.7构建信息安全运维体系

1) 掌握信息安全运维体系的内容

2) 掌握运维体系不同时期的工作内容

5.1.8建立考核与检查完善机制

5.2 安全体系设计总结

第三部分安全运行与管理

第6章 风险评估项目管理

6.1 风险评估准备工作

6.1.1组建风险评估项目团队

1) 了解直接或间接参与风险评估的角色
2) 理解参与风险评估人员的工作职责
3) 了解参与风险评估人员的关系

6.1.2制定风险评估计划

1) 掌握风险评估计划的内容
2) 掌握风险评估的过程

6.1.3识别资产

1) 理解资产的分类
2) 理解如何识别资产
3) 理解识别资产的重要性

6.1.4识别威胁

1) 理解威胁的概念
2) 掌握威胁的分类
3) 掌握威胁度量的属性
4) 掌握威胁的获取
5) 理解识别威胁的过程

6.1.5识别脆弱性

1) 理解脆弱性的概念
2) 掌握脆弱性识别的内容
3) 掌握脆弱性识别的手段
4) 理解脆弱性识别的过程
5) 掌握脆弱性的度量

6.1.6识别已有的安全措施

1) 理解安全措施的分类
2) 掌握安全措施识别的方法
3) 理解安全措施识别的过程

6.2 风险分析

6.2.1分析风险的可能性和影响

1) 掌握风险计算的公式
2) 理解风险的两个要素：可能性和后果（影响）
3) 理解风险值的计算

6.2.2风险值计算

1) 掌握风险计算模型
2) 掌握可能性计算
3) 掌握影响计算
4) 掌握风险计算

6.2.3制定风险处置计划

1) 掌握风险处理的方式

2) 理解每种方式的具体措施

6.2.4判断残余风险

1) 掌握残余风险的内涵

2) 掌握残余风险的处理

6.3 实施风险管理

6.3.1建立风险评估工作长效机制

1) 理解风险评估是一个动态的过程

2) 理解建立风险评估的长效机制

6.3.2风险管理的重要原则

1) 理解风险评估工作本身也是有风险的

2) 理解风险评估工作的原则

第7章 安全态势感知

7.1 威胁情报概念

掌握威胁情报相关概念，理解威胁情报管理模型了类型，了解收集数据与连续监控框架

7.1.1 威胁

理解威胁的概念

7.1.2情报

掌握情报定义与情报类型

7.1.3构建网络安全情报模型

掌握网络威胁情报的定义，理解攻击剖析，了解自动化

7.1.4收集数据

了解收集数据，了解联系监控框架，掌握 NIST 安全架构

7.2 威胁情报管理平台

7.2.1STIX 简介

了解 STIX 介绍

7.2.2STIX 的架构

运用 STIX 架构和每个环节的定义

7.2.3yberOX 简介

了解 CybOX 出现的必要性，理解什么是 CybOX

7.2.4CyberOX 框架

掌握 CyberOX 框架，运用 CyberOX 每个关键的定义

7.2.5TAXII 简介

理解 TAXII 架构

7.2.6TAXII 背景

掌握网络威胁信息共享模型、办法。

7.2.7 TAXII 开发方式

了解 TAXII 架构、相关规范，理解服务实现和消息数据

7.3 APT 检测技术

7.3.1APT 威胁

掌握 APT 定义、理解 PT 和 APT 的区别

7.3.2沙箱技术

1) 掌握沙箱概念，理解沙箱实现机制分析
2) 理解沙箱实现机制分析，了解基于内核级 APIHOOK 和虚拟执行的沙箱，了解 HAVE 沙箱技术

7.3.3APT 案例

掌握 APT 报告中 APT 特点和攻击范围，能通过特征定位是哪个 APT

7.4 安全信息可视化

7.4.1知识图谱

了解知识图谱的规模，知识图谱的数据来源，从抽取图谱到知识图谱

7.4.2安全数据展现

理解 Dashboard 概念，了解仪表盘的要素

7.4.3溯源

了解网络溯源面临的问题，溯源的分类，掌握大数据驱动溯源方式

第8章 安全应急管理

8.1 应急演练

8.1.1演练原则

理解演练原则指定的前提和原则的具体内容

8.1.2演练形式

1) 按组织形式划分：理解模拟演练和实战演练
2) 按内容划分：理解单项演练和综合演练
3) 按目的与作用划分：理解检验性演练、示范性演练和研究性演练

8.2 攻击排查流程

8.2.1业务异常

1. 异常类型
   1) 理解异常类型
   2) 了解异常检测原理
2. 监控异常的方法
   3) 理解应用程序日志的简述和优缺点
   4) 理解流量镜像的简述和优缺点
   5) 了解数据处理流程的简述和优缺点
   6) 了解交易异常判定的简述和优缺点

8.2.2知识域：信息泄露

理解信息泄露的危害和途径

8.3 结合各种因素制定应急预案

8.3.1基础设施因子

1. 组网环境

   理解组网环境的重要性和简述

2. 防护现状和网络防护种类

   1) 了解访问控制

   2) 了解网络隔离防护

   3) 其他措施

3. 业务类型

   了解业务系统的全面评估的重要性

4. 风险分析结论

   了解风险评估的概念和评估对象要性

8.3.2管理制度因子

理解开发人员、运维人员和第三方安全维护人员的作用和服务内容

8.4 常用检测工具介绍

8.4.1日志分析

1) 理解常见的日志类型

2) 了解常见的日志分析工具

8.4.2后门检测

1. Windows 后门检测

   1) 理解 Windows 常规检测

   2) 了解 Windows 恶意代码检测

2. UNIX/Linux 后门检测
    1) 理解 UNIX/Linux 常规检测
    2) 了解检测系统日志种类
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

8.4.3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

8.4.4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

8.5 各类事件的处置方案

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

第四部分新型安全技术与事件

第9章 新型安全技术

9.1 APT 攻击原理

9.1.1APT 攻击原理介绍

1) 了解高级持续性威胁(APT)的概念
2) 了解高级持续性威胁 APT 的内涵
3) 了解 APT 攻击的危害

9.1.2APT 攻击特点

1) 了解 APT 攻击的特点
2) 了解 APT 攻击的趋势

9.1.3APT 攻击过程

1) 了解 APT 攻击的过程
2) 了解 APT 攻击每个阶段的内容

9.1.4APT 攻击的防御

1) 了解 APT 攻击的防御方案
2) 了解每种解决方案的原理

9.2 经典 APT 攻击案例分析

9.2.1针对 Google 的极光行动

了解极光行动的过程

9.2.2夜龙行动

了解夜龙行动的过程

9.2.3海莲花

了解海莲花攻击的过程

9.3 未知特征攻击、0day 漏洞攻击介绍

9.3.10day 概念

1) 了解 0day 的概念
2) 了解漏洞发现的方法

9.3.20day 典型案例解析

1) 了解震网病毒攻击的过程
2) 了解震网病毒使用的 0day

9.3.3未知攻击的通用防御技术

1) 了解新防御方法的策略，即以“和人”为中心的安全策略
2) 了解威胁情报技术
3) 了解拟态安全

第10章 典型安全事件分析

10.1 典型安全事件分析

10.1.1 系统设计不当分析

1) 了解系统设计过程中安全的重要性
2) 了解系统设计不当案例

10.1.2 信息泄露事件分析

1) 了解典型的信息泄露事件
2) 了解信息泄露的防御方法

10.1.3 漏洞利用事件分析

1) 了解典型的高危漏洞
2) 了解应急响应的作用

10.1.4 运维管理问题

1) 了解运维管理案例
2) 了解管理措施的重要性

10.2 典型应急响应案例分析

10.2.1 Web 攻击类事件应急

1) 了解 web 攻击类事件的应急流程
2) 了解 web 攻击类事件的应急内容

10.2.2 DDOS 类事件应急

1) 了解 DDOS 类事件的应急流程

2) 了解 DDOS 攻击类事件的应急内容

10.2.3 恶意代码类事件应急

1) 了解恶意代码类事件的应急流程

2) 了解恶意代码类事件的应急内容