信息安全工程师考试大纲

一、考 试 说 明

1. 考试目标

通过本考试的合格人员能够掌握网络信息安全的基础知识和技术原理；根据国家网络信息安全相关法律法规及业务安全保障要求，能够规划、设计信息系统安全方案，能够配置和维护常见的网络安全设备及系统；能够对信息系统的网络安全风险进行监测和分析，并给出网络安全风险问题的整改建议；能够协助相关部门对单位的信息系统进行网络安全审计和网络安全事件调查；能够对网络信息安全事件开展应急处置工作；具有工程师的实际工作能力和业务水平。

2. 考试要求

（1）熟悉网络信息安全的机密性、可用性、完整性等基本知识，了解个人信息隐私保护的概念；

（2）熟悉网络信息系统的身份认证、访问控制、日志审计、安全监控工作机制和技术原理；

（3）掌握密码体制、密码算法、密码威胁、密码应用等基本知识与技术，熟悉数据加密、SSL、VPN、数字签名、PKI 等密码应用工作原理；

（4）掌握网络安全威胁工作原理，理解端口扫描、口令破解、缓冲区溢出、计算机病毒、网络蠕虫、特洛伊木马、

僵尸网络、网站假冒、拒绝服务、网络嗅探、SQL 注入等网络安全威胁相关知识；

（5）掌握防火墙、漏洞扫描、VPN、物理隔离、入侵检测、入侵防御、系统安全增强、安全审计、可信计算、隐私保护、数字水印、安全风险评估、安全应急响应等网络安全技术原理及应用；

（6）熟悉网络信息安全风险评估工作机制，了解物理环境、计算机、操作系统、数据库、应用系统、网站、智能手机、互联网、移动应用、云计算、物联网、工业控制、大数据、智能设备、机器学习等领域的安全风险，能够提出网络信息安全技术和管理解决方案，能够理解和分析评估网络安全厂商的产品技术方案；

（7）能够阅读网络信息安全等级保护标准和相关规范，能够理解相关技术标准要求；

（8）能够阅读和理解网络信息安全相关的法律法规、管理规定；

（9）熟练阅读和正确理解网络信息安全相关领域的科技英文资料，了解物联网、云计算、人工智能、大数据等新兴技术的网络安全风险。

3. 考试科目设置

（1）网络信息安全基础知识和技术，考试时间为 150 分钟，笔试，选择题；

（2）网络信息安全工程与综合应用实践，考试时间为 150 分钟，笔试，问答题。

二、考试范围

考试科目 1：网络信息安全基础知识和技术

1. 网络信息安全概述

1.1 网络信息安全基本属性

- 机密性
- 完整性
- 可用性
- 抗抵赖性
- 可控性
- 其他（真实性、时效性、合规性、隐私性、公平性等）

1.2 网络信息安全现状与问题

- 网络信息安全现状
- 网络信息安全问题

1.3 网络信息安全目标与功能

- 网络信息安全目标
- 网络信息安全功能

1.4 网络信息安全基本技术需求

- 物理环境安全
- 网络信息安全认证
- 网络信息访问控制
- 网络信息安全保密与内容安全
- 网络信息安全监测与预警
- 网络信息安全漏洞扫描与安全评估

- 恶意代码监测与防护
- 网络信息安全应急响应

1.5 网络信息安全管理内容与方法

- 网络信息安全管理目标
- 网络信息安全管理对象
- 网络信息安全管理要素
- 网络信息安全管理依据
- 网络信息安全管理方法
- 网络信息安全管理流程
- 网络信息安全管理工具

1.6 网络信息安全法律与政策文件

- 国家网络空间安全战略
- 网络信息安全基本法律
- 网络安全等级保护
- 国家密码管理制度
- 网络产品和服务审查
- 互联网域名安全管理
- 工业控制信息安全制度
- 个人信息和重要数据保护制度
- 网络安全标准规范与测评
- 网络安全事件与应急响应制度

1.7 网络信息安全科技信息获取

- 网络信息安全会议
- 网络信息安全期刊
- 网络信息安全网站
- 网络信息安全术语

2. 网络攻击原理与常用方法

2.1 网络攻击概述

- 网络攻击概念
- 网络攻击模型
- 网络攻击发展演变

2.2 网络攻击一般过程

- 隐藏攻击源
- 收集攻击目标信息
- 挖掘漏洞信息
- 获取目标访问权限
- 隐蔽攻击行为
- 实施攻击
- 开辟后门
- 清除攻击痕迹

2.3 网络攻击常见技术方法

- 端口扫描
- 口令破解
- 缓冲区溢出
- 恶意代码（计算机病毒、网络蠕虫、特洛伊木马等）
- 网站假冒
- 网络钓鱼
- 拒绝服务
- 网络嗅探
- 网络窃听
- SQL 注入攻击
- 社交工程方法

- 会话劫持
- 漏洞扫描
- 代理技术
- 数据加密技术

2.4 黑客常用软件

- 扫描类软件
- 远程监控类软件
- 密码破解类软件
- 网络嗅探类软件

2.5 网络攻击案例

- 网络端口扫描
- DoS/DDoS
- 恶意代码
- 操作系统攻击
- 数据库攻击
- 网站及 Web 应用攻击

3. 密码学基本理论

3.1 密码学概况

- 密码学发展简况
- 密码学基本概念
- 密码安全性分析

3.2 密码体制分类

- 私钥密码体制
- 公钥密码体制
- 混合密码体制

3.3 常用密码算法

- DES 密码算法

- IDEA 密码算法
- AES 密码算法
- RSA 密码算法
- 国产密码算法

3.4 Hash 函数与数字签名

- Hash 函数的工作原理
- 常见的 Hash 算法
- 数字签名的概念及作用
- 数字签名的工作原理
- 数字签名的相关算法

3.5 密码管理与数字证书

- 密码管理
- 数字证书

3.6 安全协议

- SSL
- SSH
- Diffie–Hellman 密钥交换协议

3.7 密码学网络安全应用

- 密码技术主要应用场景类型
- 路由器安全应用
- 网站安全应用
- 电子邮件安全应用

4. 网络安全体系与网络安全模型

4.1 网络安全体系概述

- 网络安全体系概念
- 网络安全体系特征
- 网络安全体系用途

4.2 网络安全体系相关安全模型

- BLP 机密性模型
- BiBa 完整性模型
- 信息流模型
- 信息保障模型
- 能力成熟度模型
- 纵深防御模型
- 分层防护模型
- 等级保护模型
- 网络生存模型

4.3 网络安全体系建设原则与安全策略

- 网络安全原则
- 网络安全策略

4.4 网络安全体系框架组成和建设内容

- 网络安全体系组成框架
- 网络安全组织体系构建内容
- 网络安全管理体系构建内容
- 网络安全技术体系构建内容
- 网络安全基础设施及网络安全服务构建内容
- 网络信息科技与产业生态构建内容
- 网络安全教育与培训构建内容
- 网络安全标准与规范构建内容
- 网络安全运营与应急响应构建内容
- 网络安全投入与建设构建内容

4.5 网络安全体系建设参考案例

- 网络安全组织体系建设参考案例
- 网络安全管理体系建设参考案例

- 网络安全技术体系建设参考案例
- 网络安全等级保护体系
- ISO 27000 信息安全管理标准

5. 物理与环境安全技术

5.1 物理安全概念与要求

- 物理安全概念
- 物理安全要求

5.2 物理环境安全分析与防护

- 自然灾害防护（防水、防雷、防震等）
- 人为破坏及鼠虫害安全防护
- 电磁及供电安全防护（防电磁、防静电、安全供电等）

5.3 机房安全分析与防护

- 机房组成内容
- 机房安全等级
- 机房场地选择

5.4 网络通信线路安全分析与防护

- 网络通信线路安全分析
- 网络通信线路安全防护

5.5 设备实体安全分析与防护

- 设备实体安全分析
- 设备实体安全防护

5.6 存储介质安全分析与防护

- 存储介质安全分析
- 存储介质安全防护

6. 认证技术原理与应用

6.1 认证概述

- 认证概念
- 认证依据
- 认证原理

6.2 认证类型与认证过程

- 单向认证
- 双向认证
- 第三方认证

6.3 认证技术方法

- 口令认证技术
- 智能卡技术
- 基于生物特征认证技术
- Kerberos 认证技术
- 公钥基础设施（PKI）技术
- 单点登录

6.4 认证主要技术指标与产品

- 认证主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 认证产品（认证产品工作机制分析、认证产品标准理解、认证产品适用场景等）

6.5 认证技术应用

- 用户身份验证
- 信息来源证实
- 信息安全保护

7. 访问控制技术原理与应用

7.1 访问控制概述

- 访问控制概念
- 访问控制目标

7.2 访问控制模型

- 访问控制模型组成要素（主体、客体、参考监视器、访问控制数据库、审计库）
- 访问控制模型运行机制

7.3 访问控制类型

- 自主访问控制
- 强制访问控制
- 基于角色的访问控制

7.4 访问控制策略设计与实现

- 访问控制策略（访问控制策略定义、访问控制策略实现、访问控制策略类型、机密性访问策略、完整性访问策略等）
- 访问控制规则类型及实施方法（基于用户身份、基于角色、基于地址、基于时间、基于异常事件、基于服务数量等）

7.5 访问控制过程与安全管理

- 访问控制管理过程
- 最小特权管理
- 用户访问管理
- 口令管理

7.6 访问控制主要技术指标与产品

- 产品的访问控制机制分析
- 产品的主要功能指标分析
- 产品的主要性能指标分析

7.7 访问控制技术应用

- UNIX/Linux 操作系统访问控制应用
- Windows 操作系统访问控制应用

- Web 服务器访问控制应用
- 网络通信访问控制应用

8. 防火墙技术原理与应用

8.1 防火墙概述

- 防火墙概念
- 防火墙工作原理
- 防火墙安全隐患
- 防火墙发展

8.2 防火墙类型与实现技术

- 基于防火墙产品形态分类（软件防火墙、硬件防火墙）
- 基于防火墙应用领域分类（网络防火墙、Web 防火墙、工控防火墙）
- 防火墙实现技术（包过滤技术、应用服务代理技术、网络地址转换技术、Web 防火墙技术、数据库防火墙技术、工控防火墙技术、下一代防火墙技术等）

8.3 防火墙主要技术指标与产品

- 防火墙主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 防火墙产品工作机制分析、防火墙产品标准理解、防火墙产品适用场景等

8.4 防火墙技术应用

- 防火墙部署过程
- 恶意流量过滤应用
- 网站保护应用
- 网络安全区域隔离

9. VPN 技术原理与应用

9.1 VPN 概述

- VPN 概念
- VPN 工作原理
- VPN 安全服务功能

9.2 VPN 类型和实现技术

- VPN 类型（链路层 VPN、网络层 VPN、传输层 VPN 等）
- VPN 实现技术（密码算法、密钥管理、认证访问控制、IPSec 协议、SSL 协议等）

9.3 VPN 主要技术指标与产品

- VPN 主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- VPN 产品工作机制分析、VPN 产品标准理解、VPN 产品适用场景等

9.4 VPN 技术应用

- 远程安全访问
- 外部网络安全互联
- 构建内部安全专网

10. 入侵检测技术原理与应用

10.1 入侵检测概述

- 入侵检测概念
- 入侵检测模型
- 入侵检测作用

10.2 入侵检测技术

- 基于误用的入侵检测技术
- 基于异常的入侵检测技术

- 基于规范的检测方法
- 基于生物免疫的检测方法
- 基于攻击诱骗的检测方法
- 基于入侵报警的关联检测方法

10.3 入侵检测系统组成与分类

- 入侵检测系统组成
- 基于主机的入侵检测系统
- 基于网络的入侵检测系统
- 分布式入侵检测系统

10.4 入侵检测系统主要技术指标与产品

- 入侵检测主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 入侵检测产品工作机制分析、入侵检测产品标准理解、入侵检测产品适用场景等

10.5 入侵检测系统应用

- 入侵检测系统部署方法与步骤
- 主机入侵检测
- 网络系统内部入侵检测
- 网络系统外部入侵检测

11. 网络物理隔离技术原理与应用

11.1 网络物理隔离概述

- 网络物理隔离概念
- 网络物理隔离工作原理

11.2 网络物理隔离系统与类型

- 网络物理隔离系统组成
- 双向网络物理隔离系统

- 单向网络物理隔离系统
- 终端物理隔离系统

11.3 网络物理隔离机制与实现技术

- 专用计算机
- 多 PC
- 外网代理服务
- 内外网线路切换器
- 单硬盘内外分区
- 双硬盘
- 网闸
- 协议隔离技术
- 单向传输部件
- 信息摆渡技术
- 物理断开技术

11.4 网络物理隔离主要技术指标与产品

- 网络物理隔离主要技术指标（功能技术指标理解、性能技术指标理解、安全技术指标理解等）
- 网络物理隔离产品工作机制分析、网络物理隔离产品标准理解、网络物理隔离产品适用场景等

11.5 网络物理隔离应用

- 内网用户安全访问互联网
- 业务生产网与互联网隔离
- 内外网安全物理隔离
- 不同安全区域信息交换

12. 网络安全审计技术原理与应用

12.1 网络安全审计概述

- 网络安全审计概念
- 网络安全审计用途

12.2 网络安全审计系统组成与类型

- 网络安全审计系统组成
- 网络安全审计系统运行机制
- 网络安全审计系统类型（网络通信安全审计、操作系统安全审计、数据库安全审计、应用系统安全审计、运维安全审计等）

12.3 网络安全审计机制与实现技术

- 网络安全审计数据采集
  - 网络流量数据采集技术（交换机端口镜像、网络嗅探等）
  - 系统日志数据采集技术（Syslog、FTP、SNMP 等）
- 网络流量数据采集开源工具 Tcpdump 的使用
- 网络审计数据分析技术（字符串匹配、全文搜索、数据关联、统计报表、可视化分析等）
- 网络审计数据保护技术（系统用户分权管理、审计数据强制访问、审计数据加密、审计数据隐私保护、审计数据完整性保护、审计数据备份等）

12.4 网络安全审计主要技术指标与产品

- 网络安全审计主要技术指标（功能技术指

标理解、性能技术指标理解、安全技术指标理解等）

- 网络安全审计产品工作机制分析、网络安全审计产品标准理解、网络安全审计产品适用场景等

12.5 网络安全审计应用

- 网络合规使用
- 网络电子取证
- 网络安全运维保障

13. 网络安全漏洞防护技术原理与应用

13.1 网络安全漏洞概述

- 网络安全漏洞概念
- 网络安全漏洞危害（敏感信息泄露、普通用户权限提升、获取远程管理员权限、拒绝服务、服务器信息泄露、非授权访问、读取受限文件、身份假冒、口令恢复、欺骗等）
- 国家信息安全漏洞库（CNNVD）、国家信息安全漏洞共享平台（CNVD）等的漏洞标准规范

13.2 网络安全漏洞分类与管理

- 网络安全漏洞来源（非技术性安全漏洞和技术性安全漏洞）
  - 非技术性安全漏洞（网络安全责任主体不明、网络安全策略不完备、网络安全操作技能不足、网络安全监督缺失、网络安全特权控制不完备等）

  - 技术性安全漏洞（设计错误、输入验证错误、缓冲区溢出、意外情况处置错误、访问验证错误、配置错误、竞争条件、环境错误等）
- 网络安全漏洞命名规范（CVE、CNNVD、CNVD 等）
- 网络安全漏洞分类分级（CNNVD 漏洞分级方法、通用漏洞计分系统、OWASP TOP 10 Web 应用漏洞等）
- 网络安全漏洞发布（漏洞发布方式、漏洞信息发布内容等）
- 网络安全漏洞获取（漏洞信息来源、漏洞信息内容等）
- 网络安全漏洞信息来源（国家信息安全漏洞库、国家信息安全漏洞共享平台、Bugtraq 漏洞库等）
- 网络安全漏洞管理过程（网络信息系统资产确认、网络安全漏洞信息采集、网络安全漏洞评估、网络安全漏洞消除和控制、网络安全漏洞变化跟踪等）

13.3 网络安全漏洞扫描技术与应用

- 主机漏洞扫描技术
- 网络漏洞扫描技术
- Web 漏洞扫描技术
- 数据库漏洞扫描技术
- 网络安全漏洞扫描应用

13.4 网络安全漏洞处置技术与应用

- 网络安全漏洞处置技术（网络安全漏洞发现技术、网络安全漏洞修补技术、网络安全漏洞利用防范技术等）
- 网络安全漏洞处置应用(服务器安全加固、网络设备安全加固等）

13.5 网络安全漏洞防护主要技术指标与产品

- 网络安全漏洞防护产品功能技术指标理解
- 网络安全漏洞防护产品性能技术指标理解
- 网络安全漏洞防护产品安全技术指标理解
- 网络安全漏洞防护产品工作机制分析
- 网络安全漏洞防护产品标准理解
- 网络安全漏洞防护产品适用场景

14. 恶意代码防范技术原理

14.1 恶意代码概述

- 恶意代码概念与分类
- 恶意代码攻击模型
- 恶意代码生存技术
- 恶意代码攻击技术
- 恶意代码分析技术
- 恶意代码防范策略

14.2 计算机病毒分析与防护

- 计算机病毒概念与特性
- 计算机病毒组成与运行机制
- 计算机病毒常见类型与技术(引导型病毒、宏病毒、多态病毒、隐蔽病毒等）
- 计算机病毒防范策略与技术（计算机病毒检测、计算机病毒防范、计算机病毒应急响应等）
- 计算机病毒防护模式（基于单机计算机病毒防护、基于网络计算机病毒防护、基于网络分级病毒防护、基于邮件网关病毒防护、基于网关防护等）

14.3 特洛伊木马分析与防护

- 特洛伊木马概念与特性
- 特洛伊木马运行机制（特洛伊木马运行过程、特洛伊木马激活等）
- 特洛伊木马技术（特洛伊木马植入技术、特洛伊木马隐藏技术、特洛伊木马存活技术等）
- 特洛伊木马防范技术（基于查看开放端口检测特洛伊木马技术、基于重要系统文件检测特洛伊木马技术、基于系统注册表检测特洛伊木马技术、检测具有隐藏能力的特洛伊木马技术、基于网络检测特洛伊木马技术、基于网络阻断特洛伊木马技术、清除特洛伊木马技术等）

14.4 网络蠕虫分析与防护

- 网络蠕虫概念与特性
- 网络蠕虫组成部件与运行机制
- 网络蠕虫常用技术（网络蠕虫扫描技术、网络蠕虫漏洞利用技术等）
- 网络蠕虫防范技术（网络蠕虫监测与预警技术、网络蠕虫传播抑制技术、网络系统漏洞检测与系统加固技术、网络蠕虫免疫

技术、网络蠕虫阻断与隔离技术、网络蠕虫清除技术等）

14.5 僵尸网络分析与防护

- 僵尸网络概念与特性
- 僵尸网络运行机制与常用技术（通信内容加密、信息隐藏等）
- 僵尸网络防范技术（僵尸网络威胁监测、僵尸网络检测、僵尸网络主动遏制、僵尸程序查杀等）

14.6 其他恶意代码分析与防护

- 逻辑炸弹
- 陷门
- 细菌
- 间谍软件

14.7 恶意代码防护主要技术指标与产品

- 恶意代码防护主要技术指标（恶意代码检测能力、恶意代码检测准确性、恶意代码阻断能力等）
- 恶意代码防护产品（终端防护类产品、安全网关、恶意代码监测类产品、补丁管理、恶意代码应急响应等）

14.8 恶意代码防护技术应用

- 终端恶意代码防护
- 电子文档及电子邮件恶意代码防护

15. 网络安全主动防御技术原理与应用

15.1 入侵阻断技术与应用

- 入侵阻断技术原理

- 入侵阻断技术应用

15.2 软件白名单技术与应用

- 软件白名单技术原理
- 软件白名单技术应用

15.3 网络流量清洗技术与应用

- 网络流量清洗技术原理
- 网络流量清洗技术应用

15.4 可信计算技术与应用

- 可信计算技术原理
- 可信计算技术应用

15.5 数字水印技术与应用

- 数字水印技术原理
- 数字水印技术应用

15.6 网络攻击陷阱技术与应用

- 网络攻击陷阱技术原理
- 网络攻击陷阱技术应用

15.7 入侵容忍及系统生存技术与应用

- 入侵容忍及系统生存技术原理
- 入侵容忍及系统生存技术应用

15.8 隐私保护技术与应用

- 隐私保护技术原理
- 隐私保护技术应用

15.9 网络安全前沿技术发展动向

- 网络威胁情报服务
- 域名服务安全保障
- 同态加密技术

16. 网络安全风险评估技术原理与应用

16.1 网络安全风险评估概述

- 网络安全风险评估概念
- 网络安全风险评估要素
- 网络安全风险评估模式

16.2 网络安全风险评估过程

- 网络安全风险评估准备
- 网络资产识别
- 网络安全威胁识别
- 网络安全脆弱性识别
- 已有安全措施确认
- 网络安全风险计算与分析
- 网络安全风险应对措施

16.3 网络安全风险评估技术方法与工具

- 资产信息收集
- 网络拓扑发现
- 网络安全漏洞扫描
- 人工检查
- 网络安全渗透测试
- 问卷调查
- 网络安全访谈
- 审计数据分析
- 入侵监测

16.4 网络安全风险评估流程和工作内容

- 评估工程前期准备
- 评估方案设计与论证
- 评估方案实施

- 风险评估报告撰写
- 评估结果评审与认可

16.5 网络安全风险评估技术应用

- 网络安全风险评估应用场景
- OWASP 风险评估方法参考
- ICT 供应链安全威胁识别参考
- 工业控制系统平台脆弱性识别参考
- 网络安全风险处理措施参考
- 人工智能安全风险分析参考

17. 网络安全应急响应技术原理与应用

17.1 网络安全应急响应概述

- 网络安全应急响应概念
- 网络安全应急响应作用
- 网络安全应急响应相关规范

17.2 网络安全应急响应组织建立与工作机制

- 网络安全应急响应组织建立
- 网络安全应急响应组织工作机制
- 网络安全应急响应组织类型

17.3 网络安全应急响应预案内容与类型

- 网络安全事件类型与分级
- 网络安全应急响应预案基本内容
- 网络安全应急响应预案类型与参考模板

17.4 常见网络安全应急事件场景与处理流程

- 常见网络安全应急事件场景（恶意程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、自然灾害性事件等）

- 网络安全应急处理流程（安全事件报警、安全事件确认、启动应急预案、安全事件处理、撰写安全事件报告、应急工作总结等）
- 网络安全事件应急演练
  - 网络安全事件应急演练类型
  - 网络安全事件应急演练方法（如 CTF 夺旗比赛/红蓝对抗赛、网络攻防平台等）

17.5 网络安全应急响应技术与常见工具

- 访问控制（防火墙、VLAN、路由器的访问设置等）
- 网络安全评估（恶意代码检测、漏洞扫描、文件完整性检查、系统配置文件检查、网卡混杂模式检查、日志文件审查等）
- 网络安全监测
  - 网络流量监测及相关工具（TCPDump、WireShark、TCPView、netstat 等）
  - Windows 系统自身监测（系统进程管理工具——任务管理器、PsTools 等，网络连接状态检查及相关工具——netstat、net、fport 等）
  - UNIX/Linux 系统自身监测（系统进程管理工具 ps，网络连接状态检查及相关工具——netstat、lsof 等）
- 系统恢复（系统紧急启动、恶意代码清除、系统漏洞修补、文件删除恢复、系统备份容灾等）
- 入侵取证（证据信息来源、证据信息获取、证据安全保护、证据分析以及相关工具，如 grep、find、OllyDbg、GDB、strings、tracert 等）

17.6 网络安全应急响应参考案例

- 公共互联网网络安全突发事件应急预案
- 网络安全应急响应服务
- 产品安全漏洞应急响应
- “永恒之蓝”攻击的紧急处置
- 页面篡改事件处置规程

18. 网络安全测评技术与标准

18.1 网络安全测评概况

- 网络安全测评概念
- 网络安全测评发展
- 网络安全测评作用

18.2 网络安全测评类型

- 基于测评目标分类（网络信息系统安全等级保护测评、网络信息系统安全验收测评、网络信息系统安全风险测评等）
- 基于测评内容分类（技术安全测评、管理安全测评等）
- 基于实施方式分类（安全功能检测、安全管理检测、代码安全审查、网络安全渗透、信息系统攻击测试等）
- 基于测评对象保密性分类（涉密信息系统测评、非涉密信息系统测评等）

18.3 网络安全测评流程与内容

- 网络安全等级保护测评流程与内容

- 技术安全测评的主要内容（安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心）
- 管理安全测评的主要内容（安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理）

- 网络安全渗透测试流程与内容
  - 网络安全渗透测试的过程（委托受理、准备、实施、综合评估、结题五个阶段）
  - 网络安全渗透测试内容（目标系统的信息收集、漏洞扫描及发现、漏洞分析及利用验证、漏洞风险处置与修补等）

18.4 网络安全测评技术与工具

- 漏洞扫描（网络安全漏洞扫描、主机安全漏洞扫描、数据库安全漏洞扫描、Web 应用安全漏洞扫描等）
- 安全渗透（安全渗透模型、安全渗透工具等）
- 代码安全审查（源代码、二进制代码等安全符合性检查）
- 协议分析（网络协议数据的获取和分析，协议分析常用工具 TCPDump、WireShark 等）
- 性能测试（性能监测工具、开源工具 Apache JMeter 等）

18.5 网络安全测评质量管理与标准

- 网络安全测评质量管理
  - 网络安全测评质量管理内容

  - 网络安全测评质量管理参考标准
  - 网络安全测评相关机构认可管理
- 网络安全测评标准
  - 信息系统安全等级保护测评标准
  - 产品测评标准
  - 信息安全风险评估标准
  - 密码应用安全
  - 工业控制系统信息安全防护能力评估

19. 操作系统安全保护

19.1 操作系统安全概述

- 操作系统安全概念
- 操作系统安全需求
- 操作系统安全机制
- 操作系统安全技术

19.2 Windows 操作系统安全分析与防护

- Windows 操作系统安全分析（系统安全架构、系统安全机制、系统安全威胁分析等）
- Windows 操作系统安全防护（系统安全增强技术方法与流程、系统安全增强工具与产品、系统常见漏洞与解决方法等）

19.3 UNIX/Linux 操作系统安全分析与防护

- UNIX/Linux 操作系统安全分析（系统安全架构、系统安全机制、系统安全威胁分析等）
- UNIX/Linux 操作系统安全防护（系统安全增强方法和流程、系统安全增强工具与产品、系统常见漏洞与解决方法等）

19.4 国产操作系统安全分析与防护

- 国产操作系统概况
- 国产操作系统安全分析
- 国产操作系统安全增强措施

20. 数据库系统安全

20.1 数据库安全概况

- 数据库安全概念
- 数据库安全威胁
- 数据库安全隐患
- 数据库安全需求

20.2 数据库安全机制与实现技术

- 数据库安全机制（标识与鉴别、访问控制、安全审计、备份与恢复、资源限制、安全加固、安全管理等）
- 数据库加密
- 数据库脱敏
- 数据库漏洞扫描
- 数据库防火墙

20.3 Oracle 数据库安全分析与防护

- Oracle 安全概况
- Oracle 安全分析
- Oracle 安全最佳实践
- Oracle 漏洞修补

20.4 MS SQL 数据库安全分析与防护

- MS SQL 安全概况
- MS SQL 安全分析
- MS SQL 安全最佳实践
- MS SQL 漏洞修补

20.5 MySQL 数据库安全分析与防护

- MySQL 安全概况
- MySQL 安全分析
- MySQL 安全最佳实践
- MySQL 漏洞修补

20.6 国产数据库安全分析与防护

- 国产数据库概况
- 国产数据库安全分析
- 国产数据库安全增强措施

21. 网络设备安全

21.1 网络设备安全概况

- 交换机安全威胁
- 路由器安全威胁

21.2 网络设备安全机制与实现技术

- 认证机制
- 访问控制
- 信息加密
- 安全通信
- 日志审计
- 安全增强
- 物理安全

21.3 网络设备安全增强技术方法

- 交换机安全增强技术方法（配置交换机访问口令和 ACL 以限制安全登录、利用镜像技术监测网络流量、MAC 地址控制技术、安全增强等）
- 路由器安全增强技术方法（及时升级操作

系统和打补丁、关闭不需要的网络服务、禁止 IP 直接广播和源路由、增强路由器 VTY 安全、阻断恶意数据包、路由器口令安全、传输加密、增强路由器 SNMP 的安全等）

21.4 网络设备常见漏洞与解决方法

- 网络设备常见漏洞（拒绝服务漏洞、跨站伪造请求、格式化字符串漏洞、XSS、旁路、代码执行、溢出、内存破坏等）
- 网络设备漏洞解决方法（及时获取网络设备漏洞信息、网络设备漏洞扫描、网络设备漏洞修补等）

22. 网络信息安全专业英语

- 具有工程师所要求的英语阅读水平
- 理解本领域的英语术语

考试科目 2：网络信息安全工程与综合应用实践

1. 网络安全风险评估与需求分析

1.1 网络安全风险评估实践

- 操作系统安全风险评估
- 数据库系统安全风险评估
- 网络设备及通信安全风险评估
- 应用系统安全风险评估
- 数据安全风险评估
- 物理安全风险评估

1.2 网络安全数据收集与分析

- syslog 日志数据采集

- 操作系统日志安全分析
- 数据库系统日志安全分析
- 网络设备日志安全分析
- 网络安全设备日志安全分析
- 网站日志安全分析
- 网络协议分析器安装和使用
- 网络协议数据安全分析

2. 网络安全常用方案设计

2.1 操作系统安全方案设计

- Windows 系统安全增强方案
- UNIX/Linux 系统安全增强方案

2.2 网络设备及通信安全方案设计

- 网络设备安全增强方案
- 网络边界安全保护方案
- 网络通信安全保护方案

2.3 计算环境安全方案设计

- 服务器安全增强方案
- 服务器安全监控方案
- 终端安全保护方案

2.4 应用及数据安全方案设计

- 应用安全保护方案
- 数据安全保护方案

2.5 网络安全管理方案设计

- 用户身份认证及访问控制方案
- 网络安全日志数据分析方案
- 网络安全运维管理方案

3. 网络安全设备部署与使用

3.1 防火墙部署与使用

- 防火墙产品技术资料阅读
- 防火墙部署和安装
- 防火墙配置与使用

3.2 IDS/IPS 部署与使用

- IDS/IPS 产品技术资料阅读
- IDS/IPS 部署和安装
- IDS/IPS 配置与使用

3.3 网闸部署与使用

- 网闸产品技术资料阅读
- 网闸部署和安装
- 网闸配置与使用

3.4 VPN 部署与使用

- VPN 产品技术资料阅读
- VPN 部署和安装
- VPN 配置与使用

3.5 漏洞扫描部署与使用

- 漏洞扫描产品技术资料阅读
- 漏洞扫描部署和安装
- 漏洞扫描配置与使用

4. 网络信息系统安全配置与管理

4.1 操作系统安全配置与管理

- Windows 系统安全配置与管理
- Linux 系统安全配置与管理

4.2 数据库系统安全配置与管理

- Oracle 安全配置与管理

- MS SQL 安全配置与管理
- MySQL 安全配置与管理
- 国产数据库安全配置与管理

4.3 网站系统安全配置与管理

- Apache 安全配置与管理
- IIS 安全配置与管理

4.4 网络设备安全配置与管理

- 路由器安全配置与管理
- 交换机安全配置与管理

5. 网站安全需求分析与安全保护工程

5.1 网站安全威胁与需求分析

- 网站安全概念
- 网站安全分析
- 网站安全需求

5.2 Apache 安全分析与增强

- Apache 安装和配置
- Apache 安全分析
- Apache 安全机制理解及配置（文件权限设置、认证和授权、日志配置和读取、IP 地址和域名访问控制）
- Apache 安全漏洞处理办法

5.3 IIS 安全分析与增强

- IIS 安装和配置
- IIS 安全分析
- IIS 安全机制类型及配置（文件权限设置、认证和授权、日志配置和读取、IP 地址和域名访问控制）

6.2.3 云计算安全管理

- 安全策略和管理制度
- 安全管理机构和人员
- 安全管理对象

6.2.4 云计算安全运维

- 云计算环境与资产运维管理
- 云计算系统安全漏洞检查与风险分析
- 云计算系统安全设备及策略维护
- 云计算系统安全监管
- 云计算系统安全监测与应急响应
- 云计算安全运维安全措施（特权管理、远程访问安全、运维审计、容灾备份等）

6.3 云计算安全保护案例分析

- 云计算安全应用参考案例分析
- 云计算隐私保护技术措施

7. 工控安全需求分析与安全保护工程

7.1 工控系统安全威胁与需求分析

- 工业控制系统概念及组成（SCADA 系统、分布式控制系统、过程控制系统、可编程逻辑控制器、远程终端、数控机床及数控系统等）
- 工业控制系统安全威胁分析（自然灾害及环境、内部安全威胁、设备功能安全故障、恶意代码、网络攻击等）
- 工业控制系统安全隐患类型（工控协议安全、工控系统技术产品安全漏洞、工控系统基础软件安全漏洞、工控系统算法安全漏洞、工控系统设备固件漏洞、工控系统设备硬件漏洞、工控系统开放接入漏洞、工控系统供应链安全等）
- 工控系统安全需求分析（传统 IT 的安全、控制设备及操作安全、安全管理合规等）

7.2 工控系统安全保护机制与技术

7.2.1 物理及环境安全防护

- 视频监控
- 工业主机加固

7.2.2 安全分区与边界防护

- 安全分区
- 工控防火墙
- 工业控制安全隔离与信息交换系统

7.2.3 身份认证与访问控制

- 多因素认证
- 最小特权
- 避免使用默认口令或弱口令

7.2.4 远程访问安全

- 禁用高风险服务
- 安全加固
- 虚拟专用网络（VPN）
- 安全审计

7.2.5 工控系统安全加固

- 安全配置策略
- 身份认证增强
- 强制访问控制
- 程序白名单控制

7.2.6 工控安全审计

- 安全审计设备部署
- 审计数据备份
- 审计数据分析利用

7.2.7 恶意代码防范

- 防病毒软件测试及部署运行
- 防病毒和恶意软件入侵管理机制
- 重大工控安全漏洞信息获取及其补丁升级措施

7.2.8 工控数据安全

- 工业数据管理方法
- 工业数据安全保护措施（安全隔离、访问控制、加密传输与存储、定期备份等）
- 测试数据保护措施（测试数据保护类型、签订保密协议、回收测试数据等）

7.2.9 工控安全监测与应急响应

- 工控网络安全监测设备安装和使用
- 工控安全事件应急响应预案制定、演练

7.2.10 工控安全管理

- 资产管理
- 冗余配置
- 安全软件选择与管理
- 配置和补丁管理
- 供应链管理

- 落实责任

7.2.11 工控安全典型产品技术

- 工控系统防护类型产品技术原理和部署使用（工控防火墙、工控加密、工控用户身份认证、工控可信计算、系统安全加固等）
- 工控系统物理隔离类型产品技术原理和部署使用（网闸、正反向隔离装置等）
- 工控安全审计与监测类型产品技术原理和部署使用（工控安全审计和工控入侵检测系统）
- 工控安全检查类型产品技术原理和部署使用（工控漏洞扫描、工控漏洞挖掘、工控安全基线检查等）
- 工控运维和风险管控类型产品技术原理和部署使用（工控堡垒机、工控风险管理系统等）

8. 移动应用安全需求分析与安全保护工程

8.1 移动应用安全威胁与需求分析

- 移动操作系统安全分析
- 移动通信网络安全分析
- 移动应用 App 安全分析

8.2 Android 系统安全与保护机制

- Android 系统安全体系
- Android 系统安全机制（进程沙箱隔离机制、SQLite 数据库安全、应用程序签名机制、权

- 大数据网络通信安全
- 大数据用户身份认证与权限管理
- 大数据计算安全
- 大数据平台应急灾备
- 大数据审计与监控

9.2.3 大数据业务安全保护技术

- 业务授权
- 业务逻辑安全
- 敏感数据安全检查

9.2.4 大数据隐私安全保护技术

- 数据身份匿名
- 数据差分隐私
- 数据脱敏
- 数据加密
- 数据访问控制

9.2.5 大数据运营安全保护技术

- 大数据处理系统的安全维护
- 大数据处理系统安全策略更新
- 大数据处理系统安全设备配置
- 大数据处理系统安全事件监测与应急响应
- 大数据处理系统入侵检测与网络安全态势感知
- 大数据处理系统网络攻击取证
- 大数据处理系统安全审计、安全堡垒机
- 大数据处理系统容灾备份

9.2.6 大数据安全管理与标准规范

- 大数据安全等级保护及相关标准规范理解
- 大数据分类分级
- 数据跨境流动安全
- 数据备份与恢复

9.3 大数据安全保护案例分析

- 大数据安全平台及解决方案分析
- 数据安全管理方法理解
- 支付卡行业数据安全规范

三、题 型 举 例

考试科目 1：网络信息安全基础知识和技术

1. 攻击者利用 John the Ripper 工具对目标服务器进行攻击，则此攻击者所利用的方法是__（1）__。

（1）A. 会话劫持　　B. 口令破解
　　C. 端口扫描　　D. 拒绝服务

2. VPN 产品的安全实现技术主要是__（2）__。

（2）A. RFC、IPSec　　B. XML、BGP
　　C. SSL、IPSec　　D. BGP、OSPF

3. 网络中的明文传输容易造成信息泄露，为了抵御网络监听，常用的技术方法是__（3）__。

（3）A. SSL、OSPF　　B. IPSec、SNMP
　　C. SSL、IPSec　　D. OSPF、SNMP

4. Network firewalls operate at different layers of the __(4)__ and TCP/IP network models. The lowest layer at which a firewall can operate is the third level which is the network layer for the OSI model and the Internet Protocol layer for TCP/IP. At this layer a firewall can determine if a packet is from a __(5)__ source but cannot grant or deny access based on what it contains. Firewalls that operate at the highest layer, which is the application layer, know a large amount of information including the source and the packet __(6)__. Therefore, they can be much more selective in granting access. This may give the impression that firewalls functioning at a higher layer must be better, which is not necessarily the case. The lower the layer at which the packet is intercepted, the more secure the system is. If the __(7)__ cannot get past the third layer, it is impossible to gain control of the operating system.

Application level gateways or proxies operate at the application layer. Packets received or leaving cannot access services for which there is __(8)__. Stateful multilayer inspection firewalls combine aspects of the other three types of firewalls.

(4) A. OSI　　B. ISO
　　C. SMTP　　D. IDS
(5) A. active　　B. old
　　C. trusted　　D. new
(6) A. virus　　B. address
　　C. contents　　D. password
(7) A. dog　　B. bird
　　C. intruder　　D. tiger

(8) A. no proxy　　B. no OS
　　C. no VPN　　D. no Desktop

考试科目 2：网络信息安全工程与综合应用实践

试题一（10 分）

某公司网站应用架构采用 LAMP 模式，其操作系统为 Linux，Web 服务器采用 Apache HTTP，数据库是 MySQL，应用编程则为 PHP，试解决网站应用中的安全问题。

（1）已知管理员使用 Telnet 和 HTTP 远程管理网站服务器，而国家信息安全等级安全保护要求为：（5 分）

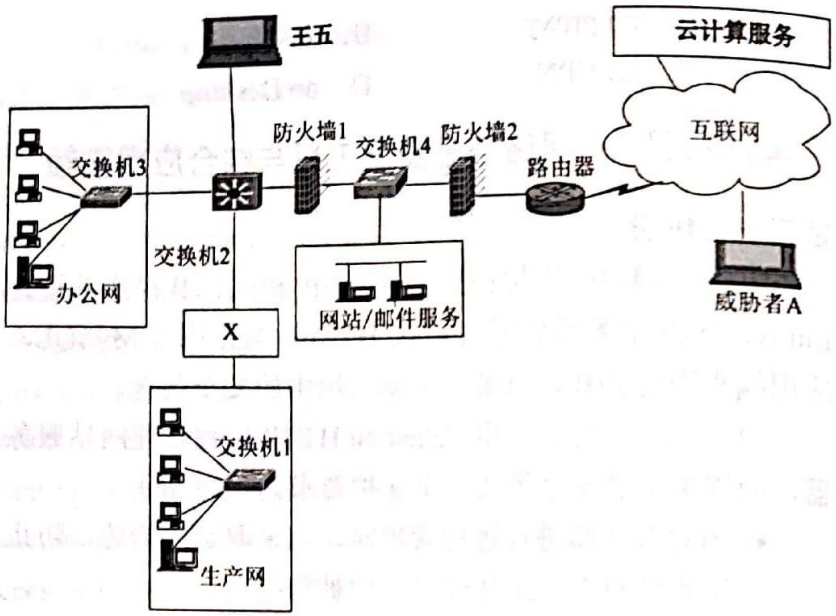
- 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。
- 应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。

请问：采取什么安全措施可以符合等级保护要求？如何获取网站操作系统和数据库的用户信息？

（2）网站安全策略要求网站的默认服务端口改成 8081，远程计算机的 IP 地址为 192.168.0.2，若要其可以访问网站服务器/www/admin 资源。如何配置 Apache 相关文件以符合安全策略要求？（5 分）

试题二（25 分）

已知甲公司网络环境结构如下图所示，请根据图中信息及问题要求，回答问题（1）至问题（4），将解答填入答题纸的对应栏内。



（1）公司为了防止生产网受到外部的网络安全威胁，安全策略要求生产网和外部网之间部署安全隔离装置，隔离强度达到接近物理隔离。请问：X 最有可能代表的安全设备是什么？简要描述该设备的工作原理。（6 分）

（2）公司拟购买云计算服务，并租用虚拟主机，请列举云计算的服务安全风险类型。（5 分）

（3）公司的防火墙是否能有效地保护虚拟主机安全？为什么？（4 分）

（4）高级持续威胁（简称 APT）常常利用电子邮件，开展有针对性的目标攻击，威胁者 A 发送带有恶意 Word 附件的电子邮件到公司邮件服务器，等待邮件接收者执行电子邮件附件，触发恶意程序运行，从而渗透到甲公司内部网络，请给出威胁者 A 的攻击流量经过的网络设备。针对 APT，可以部署什么安全设备来自动检测？该设备的主要技术方法是什么？（10 分）