安全运维实操考试内容包括

汇报人：XX　　2024-01-10

CONTENTS
目录

CHAPTER 01

考试概述与目标

考试背景与目的

适应行业发展需求

随着信息技术的快速发展，网络安全问题日益突出，对安全运维人才的需求不断增加。为了提高安全运维人员的专业技能和素质，保障企业信息系统的安全稳定运行，特设立本考试。

选拔优秀人才

通过考试选拔具有扎实的安全运维知识和实践经验的人才，为企业和机构提供高质量的安全运维服务。

考试内容与范围

安全运维基础知识

包括网络安全基本概念、常见的网络攻击手段及防御措施、密码学原理及应用等。

系统安全配置与加固

涉及操作系统、数据库、中间件等的安全配置和优化，以及漏洞扫描和修复等。

网络设备安全配置

包括路由器、交换机、防火墙等网络设备的安全配置和管理。

安全事件分析与处置

要求考生具备对安全事件进行快速响应和处置的能力，包括日志分析、恶意代码检测与清除、数据恢复等。

考试形式与时间安排

考试形式

采用闭卷笔试形式，考试时间为150分钟。

考试时间安排

每年举行两次考试，分别在6月和12月。具体考试时间和地点将在考前一个月公布。

考试费用

每次考试费用为500元/人，包括报名费、考试费、证书费等。考生需在规定时间内完成报名并缴纳费用。

CHAPTER 02

安全基础知识

网络安全基本概念

网络安全定义

网络安全是指通过采用各种技术和管理措施，保护计算机网络系统免受未经授权的访问、攻击、破坏或篡改，确保网络系统的机密性、完整性和可用性。

网络安全威胁

包括病毒、蠕虫、木马、恶意软件、钓鱼攻击、拒绝服务攻击等。

网络安全防护策略

包括防火墙、入侵检测/防御系统、加密技术、身份认证等。

常见网络攻击手段及防御措施

常见的网络攻击手段

如SQL注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、文件上传漏洞等。

安全漏洞扫描与评估

通过使用自动化工具或手动方法，发现系统中存在的安全漏洞，并进行风险评估和修复。

防御措施

包括输入验证、输出编码、权限控制、安全审计等。

密码学原理及应用

密码学基本概念

包括密码体制、加密算法、解密算法、密钥管理等。

常见加密算法

如对称加密算法（AES、DES等）、非对称加密算法（RSA、ECC等）、哈希算法（SHA-256、MD5等）。

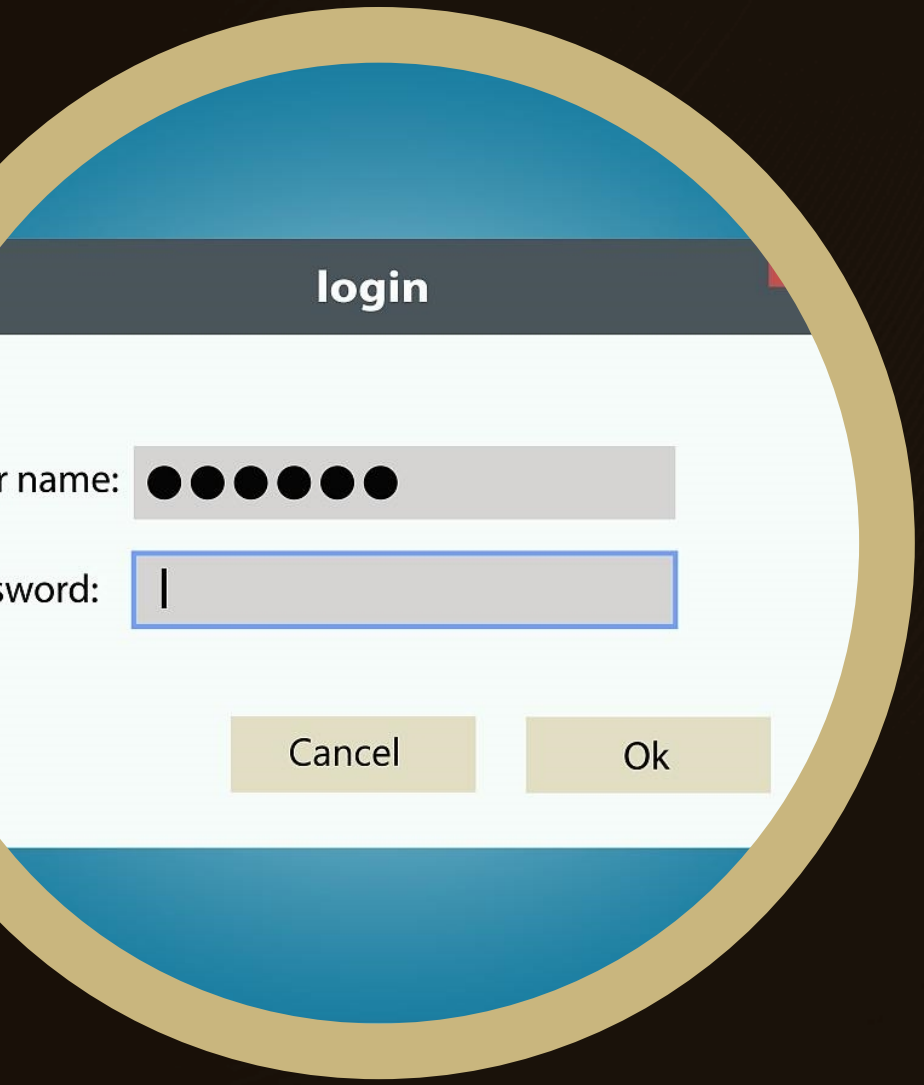
密码学应用

包括SSL/TLS协议、数字签名、电子证书等，在保障数据传输安全、身份验证等方面发挥重要作用。

CHAPTER 03

系统安全配置与加固

操作系统安全配置



01

身份鉴别

确保操作系统登录用户身份的唯一性和真实性，采用强密码策略、定期更换密码等方式提高安全性。

02

访问控制

根据用户角色和权限设置访问控制策略，防止非法用户访问系统资源。

03

安全审计

开启操作系统日志功能，记录用户操作行为，以便后续审计和分析。

数据库安全配置

- **数据库访问控制**

  设置数据库访问权限，只允许授权用户访问数据库，防止数据泄露。

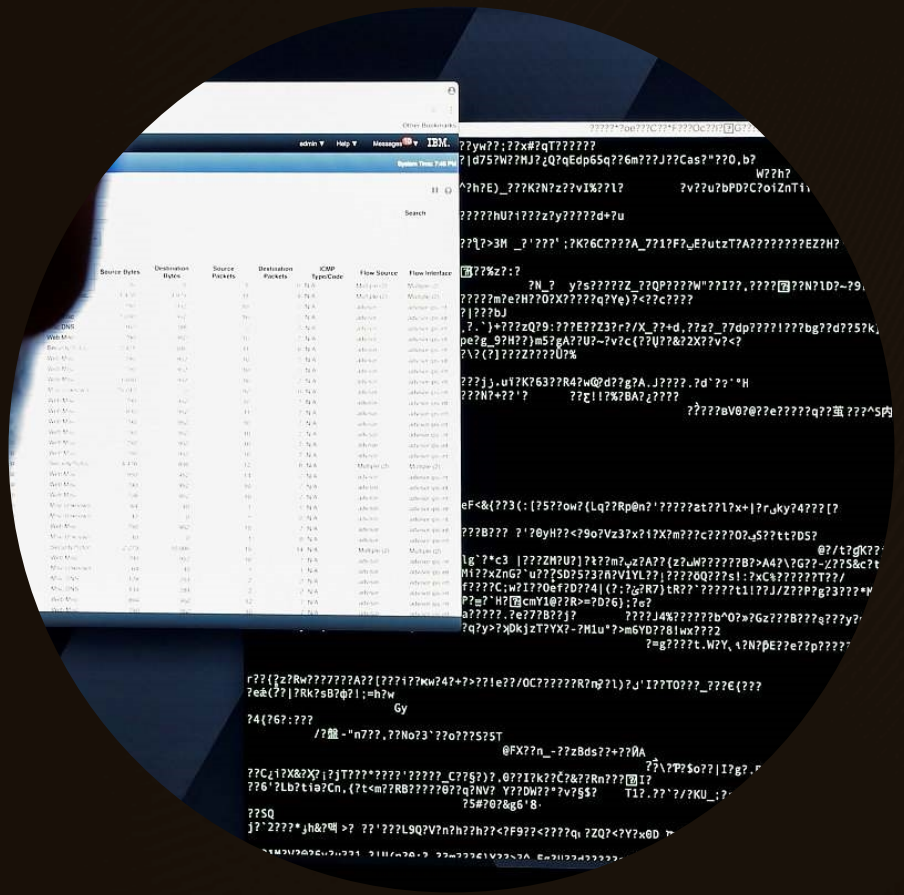
- **数据库加密**

  对敏感数据进行加密存储，确保数据在传输和存储过程中的安全性。

- **数据库备份与恢复**

  定期备份数据库，确保在发生意外情况时能够及时恢复数据。

应用系统安全加固



代码安全

采用安全的编程规范，避免代码中的安全漏洞，如SQL注入、跨站脚本等。

应用防火墙

部署应用防火墙，过滤非法请求和攻击行为，保护应用系统的安全性。

漏洞扫描与修复

定期对应用系统进行漏洞扫描，及时发现并修复潜在的安全隐患。

CHAPTER 04

网络安全设备配置与使用