# 《信息与网络安全管理》（课程代码：03345）

## 自学考试实践考核大纲

# Ⅰ课程性质与目标

## 一、课程性质和特点

“信息与网络安全管理”实践课程是面向自学考试计算机科学与工程专业设置的一门专业实践课程，是为培养学生的信息与网络安全管理素养，掌握信息与网络安全管理思想、方法及工具在实际工作中的使用，并运用掌握的信息与网络安全管理理论知识解决现实的系统安全问题而设置的一门专业实践课程。

## 二、课程目标

设置本课程的主要目的是使考生掌握信息与网络安全管理的基本理论、基本知识和基本技能，培养学生的信息与网络安全意识和能力，为未来从事相关工作打下坚实基础。

通过本课程的学习，考生应达到以下目标。

1. 理解网络信息安全的基本概念，了解网络空间面临的信息安全问题，和网络信息安全中的主要防范技术，了解网络空间信息安全的发展趋势。
2. 掌握网络空间信息密码体系，能通过密码管理策略保护信息安全。
3. 了解数字签名的实现过程和用户验证原理，能运用数字签名进行用户验证。
4. 了解网络安全协议的分类和常见网络安全协议的原理和应用。
5. 掌握无线网络通信技术，熟悉无线网络安全的防范措施。
6. 理解访问控制原理和防火墙原理，掌握网络地址转换技术和防火墙部署方法。
7. 了解网络入侵防御系统的原理和安全策略。
8. 掌握网络数据库安全技术和数据库备份技术。

## 三、与相关课程的联系与区别

本课程作为“信息与网络安全管理”理论课程对应的实践课程，主要内容为理论课程相关技术、工具在实际工作中的应用，学习本课程前需先完成对应理论课程的学习。

本课程需要计算机网路及数据库相关背景知识，学生在学习本课程前还需要掌握计算机网络技术、操作系统概论、数据库及其应用等相关课程的基本知识。

## 四、课程的重点和难点

本课程的重点内容包括：远程控制与黑客入侵、网络空间信息密码技术、数字签名与验证技术、网络安全协议、无线网络安全机制、访问控制与防火墙技术、入侵防御系统及网络数据库安全与备份技术等相关内容，以及熟练运用各种技术进行系统安全分析及设置，解决实际系统安全提升的能力。

本课程的难点内容包括：针对实际应用场景对安全需求进行分析，并根据安全需求选择合适的安全技术及工具进行实现。

## 五、考核目标

本课程的实践考核目标要求考生能运用信息与网络安全管理相关理论、技术及工具，来解决实际场景下的安全需求问题；掌握运用远程控制与黑客入侵、网络空间信息密码技术、数字签名与验证技术、网络安全协议、无线网络安全机制、访问控制与防火墙技术、入侵防御系统及网络数据库安全与备份技术等内容涉及到的技术及工具完成安全提升。

在学习本课程之前，考生应完成信息与网络安全管理课程的理论学习。

# II 课程内容与考核要求

## 第 1 章：密码相关技术及应用
## （包含教材第 4 章，第 5 章，第 6 章相关内容）

**一、课程内容**

1.1 对称密码算法设计与实现

1.2 SSL 安全协议应用

1.3 电子邮件安全

**二、学习目的与要求**

通过对本章的学习，达到如下要求：

1. 了解对称密码体系及非对称密码体系。
2. 掌握替代密码学原理及置换密码法原理。
3. 掌握数字签名及数字证书的作用。
4. 掌握基于替代密码学、置换密码学的加解密算法。
5. 掌握数字证书的生成。
6. 掌握 SSL 协议的运用。
7. 掌握 PGP 技术保证电子邮件的安全。

**三、考核知识点与考核要求**

**1. 对称密码算法设计与实现**

领会：对称密码体系；替代密码学原理；置换密码法原理。

简单应用：结合应用背景设计与实现基于替代密码学、置换密码学的加解密算法。

**2. SSL 安全协议应用**

领会：非对称密码体系；数字签名；数字证书；。

简单应用：数字证书生成

综合应用：运用 SSL 协议实现普通 Web 站点的 HTTPS 交互。

**3. 电子邮件安全**

领会：电子邮件安全协议；PGP 技术。

简单应用：运用 PGP 技术实现电子邮件的安全。

## 第 2 章：防火墙与入侵防御系统
## （包含教材第 8 章，第 9 章相关内容）

**一、课程内容**

2.1 防火墙技术

2.2 入侵防御系统

**二、学习目的与要求**

通过对本章的学习，达到如下要求：

1. 熟悉防火墙技术。
2. 掌握防火墙安全规则的实践应用。
3. 熟悉入侵检测技术。
4. 掌握入侵检测安全规则的实践应用

**三、考核知识点与考核要求**

**1. 防火墙技术**

领会：防火墙的作用；安全规则。

综合应用：根据系统需求完成防火墙安全规则的配置。

**2. 入侵防御系统**

领会：入侵检测；误用检测；异常检测。

综合应用：根据系统安全需求完成入侵检测规则的配置。

**第 3 章：网络数据库安全**

**（包含教材第 10 章相关内容）**

**一、课程内容**

3.1 数据库访问控制

3.2 数据库备份与恢复

**二、学习目的与要求**

通过对本章的学习，达到如下要求：

1. 熟悉访问控制模型。
2. 掌握数据库权限设置。
3. 熟悉数据库备份及恢复类别。
4. 掌握数据库备份及恢复技术在实践中的运用。

**三、考核知识点与考核要求**

**1. 数据库访问控制**

领会：访问控制；角色；权限。

综合应用：根据系统安全需求完成数据库角色权限设置。

**2. 数据库备份与恢复**

领会：数据库备份；数据库恢复。

综合应用：根据系统安全需求完成数据库数据的备份及恢复。

# III 关于实践考核实施的说明

一、关于能力层次的说明

在大纲的考核要求中，提出了“领会”、“简单应用”、“综合应用”等三个能力层次，它们之间是递进等级关系，后者必须建立在前者的基础上，它们的含义是：

领会：掌握课程中的基本知识点，熟悉基本的软件操作。

简单应用：掌握课程中较为深入的知识点，熟练完成较为复杂的软件操作。

综合应用：掌握课程中多个复杂知识点，并能将其结合起来，完成完整的解决方案。

二、自学教材

本实践课程使用教材为：《网络空间信息安全》，苏永红、蒋天发主编，电子工业出版社，2022 年第 2 版。

三、关于命题考试的要求

1. 本课程的命题考试，应根据本大纲所规定的考试内容和考试目标来确定范围和考核要求。考试命题适当突出重点，体现本课程综合应用的内容。

2. 本课程考试场所为计算机机房，采用现场考核方式，考生按照考核题目的要求在规定时间内完成。

3.本课程考核使用的工具：Snort、PGP Desktop、MySQL。
4.本课程考核为开卷形式，可以携带教材。
5.考核时间为 120 分钟。

**附录**

## 题型举例

**信息与网络安全管理综合题**

**1. 题目：**企业安全管理与实现

**2. 背景：**某企业有如下安全需求：

(1) 需要设计一种简单加解密算法解决明文传输的安全风险；

(2) 密钥通过邮件传输保证安全

(3) 限制企业相关软件对外网的访问

(4) 对企业数据库进行分角色授权管理

**3. 请根据上面需求，完成相关安全升级**

(1) 运用任何编程语言实现凯撒密码加解密算法，偏移量作为参数（密钥）

(2) 运用 PGP 技术把上面设置的偏移量进行邮件发送

(3) 根据要求在 Windows 自带的防火墙进行规则设置完成相关软件访问的限制

(4) 在 MySQL 中实现对不同角色的授权管理