# 2023 年硕士研究生入学考试大纲

考试科目名称: 网络与信息安全基础 考试科目代码: [837]

本考试科目考试时间 180 分钟,满分 150 分。包括计算机网络(占 60 分)、信息安全基础(占 45 分)和网络安全基础(占 45 分)三个部分。

# 计算机网络部分(60分)

#### 一、考试要求

掌握计算机网络的基本概念、基本原理和基本方法;掌握计算机网络的体系结构和典型网络协议,了解典型网络的组成和特点,理解典型网络设备的工作原理;掌握 socket 编程基本技术;能够运用计算机网络的基本概念、基本原理和基本方法进行网络系统的分析、设计和应用。

注:考试内容以参考书目1为主。

# 二、考试内容

- 1) 计算机网络体系结构的概念
  - a:报文交换基本概念
  - b: TCP/IP 体系结构
  - c: IP 地址, 子网
- 2) 应用层
  - a: Web 与 HTTP
  - b: DNS
  - c: SMTP
- 3) 传输层
  - a: UDP
  - b: TCP
  - c: 拥塞控制
- 4) socket 编程
  - a: UDP 编程
  - b: TCP 编程
  - c: 原始套接字编程

#### 5) 网络层

- a: 链路状态路由协议
- b: 距离向量路由协议
- c: BGP
- 6)链路层
  - a:ARP
  - b:WIFI
  - c: CDMA

# 三、试卷结构

- 1) 题型结构
  - a:填空题(0-15分)
  - b:选择题(0-30分)
  - c: 简答题(0-30 分)
  - d:问答题(0-30分)
  - 注: 题型分数在以上范围内浮动,总分为60分

#### 四、参考书目

- 1. James F. Kurose, and Keith W. Ross, 计算机网络-自顶向下方法(原书第6版), 机械工业出版社. 2014
- 2. 谢希仁. 计算机网络(第6版). 电子工业出版社, 2013

# 信息安全基础部分(45分)

#### 一、考试要求

要求考生全面掌握信息安全领域的基本内涵、概念、原理和方法,系统深入地理解密码学基本理论、身份认证、访问控制、计算机病毒与网络入侵、防火墙与入侵检测、安全传输协议、风险评估与控制理论、信息安全标准与法律法规,掌握信息安全服务的逻辑设计与基本技术路线,理解各种信息安全服务之间的相互关系,建立信息安全体系的整体概念。

#### 二、考试内容

- 1) 信息安全的基本概念
  - a: 信息安全知识体系结构
  - b: 信息的基本安全属性
  - c: 信息保障
  - d: 安全服务与机制
- 2) 密码学基础
  - a: 密码分类、作用与基本设计原理
  - b: 对称密钥密码与 DES
  - c: 公开密钥密码、DH 密钥交换协议与 RSA
  - d: 散列函数原理及作用
- 3) 身份认证与访问控制
  - a: 基于对称密钥的认证设计与 kerberos 协议
  - b: 基于公开密钥的认证设计与 PKI 理论
  - c: 三种典型的访问控制模型及实现机制
  - d: Windows 系统网络认证及访问控制
- 4) 计算机病毒与网络入侵
  - a: 传统计算机病毒、蠕虫病毒、木马病毒的特点、原理与防治
  - b: 拒绝服务攻击的特点及典型攻击机理
  - c: 欺骗类攻击的特点与典型攻击
  - d: 利用型攻击的特点及缓冲区溢出原理
- 5) 防火墙、入侵检测与安全传输协议
  - a: 防火墙理论与 netfilter 结构原理
  - b: 入侵检测理论与 snorts 结构原理
  - c: IPSec 与 SSL 协议的组成及工作原理
  - d: SET 协议体系与关键技术
- 6) 安全风险管理与法律法规
  - a: 信息系统风险评估与控制

b: CC 标准与 BS7799

c: 信息安全道德与法律法规

### 三、试卷题型结构

a: 填空题(0-20分)

b: 选择题(0-20分)

b: 简答题(0-30分)

c: 计算与综合设计题(0-30分)

# 四、参考书目

1、翟健宏,信息安全导论,科学出版社,2011.07

2、刘建伟等,网络安全——技术与实践,清华大学出版社,2011.07

#### 网络安全基础部分(45分)

#### 一、考试要求

掌握网络安全领域中由于各层网络协议缺陷及其引发的网络攻击、软件程序 缺陷及其引发的攻击、资源占用攻击等;掌握网络监听技术及相关网络数据获取 的软件开发能力;掌握入侵检测的相关理论和技术以及典型的模式匹配方法和分 类方法;掌握身份认证相关的模型、技术和系统。

#### 二、考试内容

1) 网络攻击

a: 各层网络协议缺陷及攻击

b: DOS 和 DDOS 攻击

c: 格式化攻击、缓冲区溢出攻击

d: Web 攻击技术

2) 网络数据获取

a: 网络数据包的捕获

b: 包捕获机制

b: WinPcap 或 Libpcap 编程

- 3) 网络扫描技术
  - a:主机发现技术
  - b:端口扫描技术
- 4)入侵检测
  - a: 入侵检测的相关概念与体系结构
  - b: 入侵检测系统的数据源
  - c: 基于误用的入侵检测
  - d: 基于异常的入侵检测
  - e: 告警与响应
- 4) 典型模式匹配算法
  - a: 单模式匹配算法: KMP、BM
  - b: 多模式匹配算法: AC、WM
- 5) 典型分类算法
  - a: K-均值算法
  - b: 支持向量机和传统 Bayes 分类方法
- 5) 身份认证技术
  - a:数字签名
  - b:报文认证
  - c:CA 中心

# 三、试卷题型结构

- a: 填空题(0-20分)
- b: 选择题(0-20分)
- b: 简答题(0-30分)
- c: 计算与综合设计题(0-30分)

# 四、参考书目

1. 吴礼发,洪征,李华波编著,网络攻防原理与技术,机械工业出版社, 2017.01 2. 薛静锋,祝烈煌主编,入侵检测技术(第2版),中国工信出版集团人民邮电出版社,2016.01