附件 3

2025 年度江西省公安机关网络安全技术职位专业科目测试和专业技能测试大纲

为便于报考人员充分了解江西省 2025 年公安机关网络安全技术职位专业科目测试和专业技能测试，特制定本大纲。

一、考试性质和目标

网络安全技术职位专业科目测试和专业技能测试是针对计算机相关学科报考人员设置的专业技术水平测试。考试主要测试报考人员的网络安全实操能力素质，包括对计算机技术、软件技术、网络安全技术等学科相关内容的掌握程度和应用相关知识解决实战问题的能力。

通过考试的人员，表明其已具备从事公安机关网络安全技术职位相应专业岗位工作的能力和水平，用人单位可根据工作需要从通过人员中择优安排从事公安机关网络安全相关技术工作。

二、考试方式和时限

专业科目测试采用闭卷笔试考试方式，全部为客观性试题，考试时限 90 分钟，满分 100 分。

专业技能测试为计算机实机操作。考试时间为 150 分钟，满分 100 分。

考试上机环境为 Windows 10，虚拟机环境为 Kali Linux，集

成开发环境（IDE）为 Visual Studio、 Eclipse、PyCharm 等。

三、考试内容

本大纲规定了每一个知识要点的内容和深度要求，分为“了解”“理解”和“掌握”三类:

了解: 是最低限度要求，报考人员需要正确认识该知识要点的基本概念和原理，大纲内未作特别标注的都为了解性要求。

理解（用“★”标注）：是中等深度要求，报考人员需要在正确认识该知识要点的基本概念和原理的基础上，深入理解其内容，并可以进一步地判断、推理，能通过计算机操作完成相关题目。

掌握（用“★★”标注）：是最高深度要求，报考人员需要正确认识该知识要点的概念、原理，并在深入理解的基础上灵活运用、举一反三，并能熟练通过计算机操作完成相关题目。

第一编　法律法规基础知识

（一）网络安全相关法律法规

1. 《中华人民共和国网络安全法》

2. 《中华人民共和国数据安全法》

3. 《中华人民共和国个人信息保护法》

4. 《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》（法发〔2022〕23 号）

5. 《公安机关办理刑事案件电子数据取证规则》

第二编　计算机专业基础知识

（二）计算机组成原理

1. 计算机硬件的发展历程
2. 计算机软件的分类
3. 计算机硬件的基本组成
4. 计算机软件和硬件的关系
5. 计算机的工作过程
6. ★计算机的性能指标
7. ★进位计数制及其相互转换
8. ★字符和字符串
9. 浮点数的表示和运算
10. 存储器的分类
11. 存储器的性能指标
12. 虚拟存储器
13. ★指令的基本格式
14. ★常见数据寻址方式
15. CISC 和 RISC 的基本概念
16. CPU 的功能和基本结构
17. 总线标准
18. ★★常见编码的识别与转换

(1) ASCII 编码

(2) Base64 编码

(3) shellcode 编码

(4) Quoted-printable 编码

(5) XXencode 编码

(6) UUencode 编码

(7) URL 编码

(8) Unicode 编码

(9) Escape/Unescape 编码

(10) HTML 实体编码

(11) 莫尔斯电码（Morse Code）

（三）操作系统

1. 操作系统的基本概念

2. 操作系统的主要功能和提供的服务

3. 操作系统的分类

4. ★进程与线程

5. 处理器的调度

6. ★内存管理，熟悉获取内存数据的方法，可以使用工具将当前主机内存保存为镜像文件。

7. ★文件管理

8. ★设备管理

9. ★磁盘阵列的主要实现方式

10. ★★Linux 基础

(1) 常用基础命令

(2) 根目录结构

(3) 进程管理

(4) UID 和 GID

(5) 权限设置

(6) procfs 文件系统

(7) 用户管理

(8) 引导和启动

(9) 基于关键词或者属性条件对文件进行过滤，基于字符串或正则表达式对文件内容进行数据搜索。

11. ★★Windows 基础

(1) Windows 的版本

(2) 引导和启动

(3) 用户管理

(4) 文件系统

(5) 服务

(6) 通过注册表对文件和历史记录进行搜集和痕迹分析

(7) 进程管理

(8) 设备管理

（四）计算机网络

1. 计算机网络的组成

2. 计算机网络的分类

3. ★计算机网络体系结构与参考模型

4. 物理层

(1) 数据传输方式

(2) 传输介质分类

(3) 物理层设备

(4) 数据链路层

(5) 局域网的基本概念与体系结构

(6) ★以太网的工作原理

(7) 以太网的 MAC 帧

(8) 以太网的传输介质

(9) 无线局域网

(10) 广域网

(11) 数据链路层设备

(12) 虚拟局域网（VLAN）

5. 网络层

(1) 子网划分和无分类编址 CIDR

(2) 路由算法

(3) ★IP 地址的分类、IP 数据报格式、NAT

(4) ★ARP、DHCP 和 ICMP

(5) ★3 种常用路由选择协议：RIP、OSPF、BGP

(6) IP 组播、移动 IP 的基本概念

(7) 路由器的组成和功能

(8) ★IPV6

6. 传输层

(1) TCP 的流量控制和拥塞控制机制

(2) ★TCP 报文格式

(3) ★UDP 数据报格式

7. ★★应用层

(1) 域名解析过程

(2) FTP 的工作原理

(3) HTTP 抓包与调试

(4) Fiddler 的使用与操作

(5) Wireshark 的使用与操作

(6) 服务端跳转

(7) 客户端跳转

(8) 常见搜索引擎高级语法的使用

(9) HTTP 请求与响应

(10) HTTP 的请求方法

(11) URL 的特征分析

(12) HTTP 消息头

(13) HTTP 状态码

(14) 使用浏览器执行前端 JavaScript

(15) 使用 Node.js 执行后端 JavaScript

第三编　数据科学基础知识

（五）★★Python 编程基础

1. 基础语法与概念

(1) 基本数据类型（整型、浮点型、字符串、布尔型）

(2) 变量与赋值

(3) 输入与输出（print 函数和 input 函数）

2. 控制结构

(1) 条件语句（if，elif，else）

(2) 循环结构（while 循环，for 循环）

(3) 循环控制语句（break，continue）

(4) 简单列表推导式

3. 数据结构

列表（List）、元组（Tuple）、字典（Dictionary）、集合（Set）、数据结构的相关操作和方法

4. 函数与模块

(1) 函数定义与调用

(2) 参数传递与返回值

(3) 局部变量与全局变量

(4) 匿名函数（lambda 表达式）

(5) 模块的使用（import 语句）

(6) 常用标准库模块（如 math，datetime）

5. 面向对象编程

(1) 类与对象的概念

(2) 类的定义与对象的创建

(3) 实例属性与方法

(4) 类属性与类方法

(5) 继承与多态

(6) 特殊方法（如__init__，__str__等）

6. 异常处理

(1) 异常的概念

(2) try-except 语句

(3) 处理多种异常

(4) finally 子句

(5) 自定义异常

7. 文件与输入输出

(1) 文件的打开与关闭

(2) 读取与写入文件

(3) 文件上下文管理器（with 语句）

(4) 文件的其他操作（如删除、重命名）

8. 高级主题

(1) 上下文管理器与 with 语句

(2) 正则表达式和 GREP 语法

(3) 数据科学相关库（如 NumPy，Pandas）

（六）数据库管理与 SQL

1. 数据库系统的基本概念

2. 数据库的分类和常见数据库软件

3. SQL 的特点

4. ★★使用 SQL 语言完成对数据库的查询、插入、删除、更新操作，可以用 SQL 语言正确完成复杂查询操作。

(1) 查询多个列

(2) 查询去重

(3) SQL 聚合函数

(4) SQL 字符串函数

(5) SQL 数值函数

(6) SQL 日期和时间函数

(7) SQL 数据分组

5. ★★常见数据库的备份操作

6. ★★通过数据库日志恢复数据

7. ★常见数据库的客户端工具的使用

8. ★★能够在 MySQL、SQLite 上通过编程的方式开发应用程序，完成对数据库的各种操作；能够使用 ODBC、JDBC 进行数据库应用程序的设计。

9. ★★数据库连接地址、连接口令的分析方法

（七）★数据结构与算法基础

1. 二叉树的定义及其主要特征

2. 二叉排序树

3. 赫夫曼（Hoffman）树和赫夫曼编码

4. 树和森林的遍历

5. 图的基本概念

6. 图的遍历算法

7. 普里姆算法和克鲁斯卡尔算法

8. 迪杰斯特拉算法

9. 弗洛伊德算法

10. 关键路径核心算法

11. 拓扑排序核心算法

12. 排序算法

13. 顺序查找算法

14. 折半查找算法

15. 二排序树的基本算法

16. B-树的基本概念和操作

17. B+树的基本概念和操作

（八）数据分析与挖掘的基础方法

1. ★★关键字搜索方法

(1) GREP 语法

(2) 关键字的编码

2. ★★使用 EXCEL 或者 WPS 进行数据分析

(1) 单元格格式调整方法

(2) 数据查找和替换方法

(3) 外部数据导入导出方法

(4) 数据有效性检查方法

(5) 日期和时间格式的处理方法

(6) 数据筛选和排序

(7) 数据分类汇总

(8) 数据透视表、图的使用，包括分类汇总、取平均、最大最小值、自动排序、自动筛选、自动分组；可分析占比、同比、环比、定比。

(9) EXCEL 两表数据比对方法

(10) EXCEL 常用统计公式使用

(11) 日期函数：day，month，year，date，today，weekday，weeknum。

(12) 数学函数：product，rand，randbetween，round，sum，sumif，sumifs，sumproduct。

(13) 统计函数：large，small，max，min，median，mode，rank，count，countif，countifs，average，averageif。

(14) 查找和引用函数：choose，match，index，indirect，column，row，vlookup，hlookup，lookup，offset，getpivotdata。

(15) 文本函数：find，search，text，value，concatenate，left，right，mid，len。

(16) 逻辑函数：and，or，false，true，if，iferror。

3. ★★文本编辑器数据处理

(1) 列编辑模式的使用

(2) 各类编码字符的搜索和替换

(3) 正则搜索语法

4. ★★数据清洗，使用 Python 对乱码，错位，重复值，未匹配等脏数据进行补全、删除等一致化处理。

第四编　网络安全基础知识

（九）★★网络安全基础

1. 流量分析识别网络安全威胁

(1) 端口扫描与监听

(2) 口令破解

(3) 拒绝服务攻击

(4) 漏洞攻击（缓冲区溢出、系统漏洞、应用软件漏洞）

(5) 僵尸网络

(6) 网络钓鱼

(7) 网络欺骗

(8) 网站安全威胁的识别（SQL 注入漏洞、跨域攻击、命令执行漏洞、文件漏洞等）

2. 使用 Web 编程语言发现和测试漏洞

3. 主流渗透测试和漏洞扫描工具的使用

4. 熟悉 SQL 注入、跨站脚本、文件上传、文件包含、CSRF、SSRF、命令执行、反序列化等 web 漏洞的原理与利用方式，会使用程序工具或技术方法检测。掌握主流 Web 中间件的常见安全隐患检测及加固方式，包括但不限于 Struts2、jBoss、WebLogic、FastCGI、PHPCGI。

5. 掌握 Web 服务的安全隐患检测及加固方式，包括但不限

于: IIS 服务器漏洞、Apache 服务器漏洞、Nginx 服务器漏洞、Tomcat 服务器漏洞。

6. 熟悉主流网站服务器操作系统的的安全隐患检测及加固方式，包括但不限于 Windows、Linux 等。

7. 通过恶意代码、文件传播方式溯源攻击路径

8. 通过 Apache、IIS 日志分析网络入侵行为

9. 利用系统日志、应用程序、安全日志等排查和溯源攻击行为

10. 对内存数据进行分析，熟悉使用工具提取下列信息:

(1) 进程信息，如进程名称、进程 ID、线程信息等。

(2) 网络连接，如 IP 地址、端口号、连接状态等。

(3) 文件信息，如文件名、文件路径、文件大小等。

(4) 注册表信息，如键值、权限设置等。

(5) 系统信息，如操作系统版本、硬件配置等。

11. 掌握 Linux 系统磁盘数据调查分析，Windows 系统磁盘数据调查分析的能力。

12. 关系型和非关系型数据库安全检测与防护，包括 Mysql、SQL Server、Oracle 等常见数据库的库表查询管理、用户权限管理、备份还原等基础技术；数据库入侵防护、访问控制、身份认证、数据加密等安全措施；常用数据库管理客户端程序使用、应用系统访问和重要操作审计等。

（十）★★逆向工程

1. Android 逆向分析。掌握 APK 解包工具的使用；掌握使用 IDA、JEB 等工具对 ELF、DEX 文件进行动态调试和静态分析的能力，能够快速定位关键逻辑，理解 x86、arm 汇编、smali 代码翻译成用语言描述的逻辑说明或可以编译的高级语言代码；能够对低对抗性加壳文件进行脱壳；能够对典型打包框架进行分析处理。

2. Windows 逆向分析。掌握使用 IDA、Ollydbg、Windbg、x64Dbg 等工具对 PE 文件进行动态调试和静态分析的能力，能够快速定位到关键逻辑，理解 x86 汇编代码翻译成用语言描述的逻辑说明或可以编译的高级语言代码；能够对低对抗性加壳文件进行脱壳。

3. Linux 逆向分析。掌握使用 IDA、GDB 等工具对 ELF 文件进行动态调试和静态分析的能力，能够快速定位到关键逻辑，理解汇编代码翻译成用语言描述的逻辑说明或可以编译的高级语言代码；能够对低对抗性加壳文件进行脱壳。

4. 恶意程序（代码）的识别及防护。运用相关工具或技术方法发现、隔离、清除常见恶意程序（代码），包括远程控制木马、后门程序、Webshell 等；并能对常见恶意程序（代码）进行混淆还原和逆向分析。

（十一）★加密与解密

1. 加密解密原理

(1) Hash 算法和数字签名原理

(2) 对称与非对称加密算法原理

(3) 字典穷举原理

(4) 彩虹表原理

(5) 常用的解密站点与工具

2. 加密文件的识别、查找方法

(1) 常见“哈西+盐”的特征和识别方法

(2) 常见文件加密工具的特点和识别方法

(3) 常见磁盘加密的特点和识别方法

3. 密码破解技术及工具的使用方法

(1) 暴力破解技术及工具

(2) 基于数据字典破解技术

(3) 基于社会工程学破解技术

(4) 数据库密码破解

(5) Windows 的密码移除

4. 代码混淆加密与解密

(1) asp 混淆加密

(2) php 混淆加密

(3) css/js 混淆加密

(4) VBScript.Encode 混淆加密

(5) ppencode

(6) rrencode

(7) jjencode/aaencode

(8) JSfuck

(9) jother

（十二）★★数据分析

1. 比对分析。掌握 Excel 中数据对比常用的方法，包括但不限于：简单的直接等式对比、使用 Vlookup 函数进行数据的匹配对比、使用数据透视进行数据对比、用 PowerQuery 实现表间数据的自动对比、熟悉 Excel 条件格式比对法和函数对比法。

2. 统计分析。掌握常用的数据统计方法，包括但不限于对比分析、分组分析、预测分析、漏斗分析、聚类分析、因子分析、相关分析、对应分析、回归分析、方差分析。

3. 数据清洗。掌握从目标数据中发现并纠正残缺数据、错误数据、重复数据等错误，检查数据一致性，处理无效值和缺失值等。