附件4

2022年度广西壮族自治区公安机关大数据职位专业科目笔试和专业技能测试大纲

为便于应试者充分了解广西壮族自治区公安机关大数据职位专业科目笔试和专业技能测试，制定本大纲。

一、考试性质和目标

公安机关大数据职位专业科目笔试和专业技能测试是针对计算机科学与技术类考生设置的专业能力考试科目。主要测试考生的大数据能力素质，包括对计算机科学与技术类学科各项内容的掌握程度和应用相关知识解决问题的能力。

通过本考试的合格人员能根据应用部门的要求进行大数据系统的规划、设计，能进行大数据系统的运行、维护、管理，能高效、安全地管理网络资源；对大数据系统开发进行业务指导，具有较强的大数据应用和管理能力；熟悉数据搜集、整理、分析，并依据数据做业务研究、评估和预测的专业人员。

二、考试方式和时限

加试专业科目笔试和专业技能测试，其中专业科目笔试采取闭卷笔试方式进行，分为客观性试题和主观性试题两部分，考试时间为120分钟，满分100分。

专业技能测试方式为计算机实机操作，参照在线解题模式CTF（Capture The Flag）赛制，考试时间为180分钟，满分100分。考生使用机试环境提供的工具、数据、考试平台进行在线答题。在解题模式CTF赛制中，考生可以通过考场现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决竞赛题目的分值和时间来记分和排名，每个题目根据难度不同有不同分值。上机环境为Windows 10和Kali双系统，集成开发环境（IDE）为Visual Studio、 Eclipse、PyCharm。

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：是最低深度要求，考生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，考生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，并可以进一步的判断、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，考生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。

（一）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)

（二）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

7.★★文件管理

8.★设备管理

9.★磁盘阵列

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

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)注册表

(7)进程管理

(8)设备管理

(9)日志与日志文件

（三）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

（四）数据库系统

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

（五）★数据结构与算法

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

（六）★网络安全基础

1.流量分析识别网络安全威胁

(1)网络监听

(2)口令破解

(3)拒绝服务攻击

(4)漏洞攻击（缓冲区溢出原理、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（SQL注入漏洞、跨域攻击、命令执行漏洞、文件漏洞等）

2.常见漏洞的利用方法

3.主流渗透测试和扫描工具的使用

4.主流数据库语句以及SQL注入漏洞手工测试及绕过方法

5.常见的漏洞原理和利用方式

6.主流中间件的常见安全隐患及加固方式

7.恶意代码、文件传播方式判断和路径追溯

8.通过Apache、IIS日志分析网络入侵行为

9.XSS漏洞手工测试方法

（七）★★数据分析与挖掘

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

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。

（八）★逆向工程

1.Android、IOS调试、逆向工具使用

(1)apktool, jd-gui等安卓APK的反编译与加壳、动态调试技术

(2)熟悉IOS ipa文件的反编译，动态调试

2.IDA、WinDbg、OllyDbg、PEID等调试、逆向工具的使用

（九）★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

四、题型样例

（一）选择题（单选、多选题）

传输一幅分辨率为 640 像素 480 像素、65536 色的图片（采用无压缩方式），假设采用数据传输速率为 56kbits，大约需要的时间是（）。A.34.82s B.42.86s C.85.71 D.87.77s

（二）填空题

1.查看当前Linux系统内安装的web服务版本。

2.网管小王在上网途中发现自己的网络访问异常缓慢，于是对网络出口捕获了流量（goodluck.pcapng），请您分析流量后进行回答。此时正在进行的可能是\_\_\_\_\_\_\_\_\_\_协议的网络攻击。

（三）编程题

某百货公司为了促销，采用购物打折的优惠方法，每位顾客一次购物：在 1000 元以上者，按 9.5 折优惠；在 2000 以上者，按 9 折优惠：在 3000 以上者，按 8.5 折优惠；在 5000 以上者，按 8 折优惠；编写程序，输入购物款数，计算并输出优惠价。

（四）简答题

1.什么是多线程？多线程与多任务有什么区别？

2.当用户在Web览器中输入域名“www.goodluck.com”访问该网站时，可能会依次发送哪些报文？