附件3

2024年度广西壮族自治区公安机关

网络安全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广西壮族自治区2024年公安机关网络安全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犯罪侦查取证、网络安全监管与执法、情报信息搜集与分析、网络安全攻防对抗等专业技术工作。

二、考试方式和时限

**专业科目测试**采用闭卷笔试考试方式，分为客观性试题和主观性试题两部分，考试时限120分钟，满分100分。

**专业技能测试**为计算机实机操作，类似解题模式的CTF竞赛，通过完成下列类似任务来获得分值，如分析指定文件中的一系列数据、在指定的靶场环境（虚拟机、容器）中找到隐藏的“旗帜”（flags）、完成指定任务的操作并反馈结果、编写代码并运行后反馈结果。完成实机操作后，必须按照要求完成电子答卷提交，考官阅卷评分以报考人员提交的电子答卷及附件文件为准。考试时间为180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

1. 网络安全相关法律法规
2. 《中华人民共和国网络安全法》
3. 《中华人民共和国数据安全法》
4. 《中华人民共和国个人信息保护法》
5. 《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）
6. 《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

1. 计算机组成原理
2. 计算机硬件的发展历程
3. 计算机软件的分类
4. 计算机硬件的基本组成
5. 计算机软件和硬件的关系
6. 计算机的工作过程
7. ★计算机的性能指标
8. ★进位计数制及其相互转换
9. ★字符和字符串
10. 浮点数的表示和运算
11. 存储器的分类
12. 存储器的性能指标
13. 虚拟存储器
14. ★指令的基本格式
15. ★常见数据寻址方式
16. CISC和 RISC 的基本概念
17. CPU 的功能和基本结构
18. 总线标准
19. ★★常见编码的识别与转换
20. ASCII编码
21. Base64编码
22. shellcode编码
23. Quoted-printable编码
24. XXencode编码
25. UUencode编码
26. URL编码
27. Unicode编码
28. Escape/Unescape编码
29. HTML实体编码
30. 莫尔斯电码（Morse Code）
31. 操作系统
32. 操作系统的基本概念
33. 操作系统的主要功能和提供的服务
34. 操作系统的分类
35. ★进程与线程
36. 处理器的调度
37. ★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。
38. ★文件管理
39. ★设备管理
40. ★磁盘阵列的主要实现方式
41. ★★Linux基础
42. 常用基础命令
43. 根目录结构
44. 进程管理
45. UID 和 GID
46. 权限设置
47. procfs文件系统
48. 用户管理
49. 引导和启动
50. 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
51. ★★Windows基础
52. Windows的版本
53. 引导和启动
54. 用户管理
55. 文件系统
56. 服务
57. 通过注册表对文件和历史记录进行搜集和痕迹分析
58. 进程管理
59. 设备管理
60. 计算机网络
61. 计算机网络的组成
62. 计算机网络的分类
63. ★计算机网络体系结构与参考模型
64. 物理层
65. 数据传输方式
66. 传输介质分类
67. 物理层设备
68. 数据链路层
69. 局域网的基本概念与体系结构
70. ★以太网的工作原理
71. 以太网的 MAC 帧
72. 以太网的传输介质
73. 无线局域网
74. 广域网
75. 数据链路层设备
76. 虚拟局域网（VLAN）
77. 网络层
78. 子网划分和无分类编址 CIDR
79. 路由算法
80. ★IP 地址的分类、IP 数据报格式、NAT
81. ★ARP、DHCP 和 ICMP
82. ★3 种常用路由选择协议：RIP、OSPF、BGP
83. IP 组播、移动 IP 的基本概念
84. 路由器的组成和功能
85. ★IPV6
86. 传输层
87. TCP 的流量控制和拥塞控制机制
88. ★TCP 报文格式
89. ★UDP 数据报格式
90. ★★应用层
91. 域名解析过程
92. FTP 的工作原理
93. HTTP抓包与调试
94. Fiddler的使用与操作
95. Wireshark的使用与操作
96. 服务端跳转
97. 客户端跳转
98. 常见搜索引擎高级语法的使用
99. HTTP 请求与响应
100. HTTP 的请求方法
101. URL的特征分析
102. HTTP 消息头
103. HTTP状态码
104. 使用浏览器执行前端 JavaScript
105. 使用 Node.js 执行后端 JavaScript

第三编 数据科学基础知识

1. ★★Python编程基础
2. 基础语法与概念
3. 基本数据类型（整型、浮点型、字符串、布尔型）
4. 变量与赋值
5. 输入与输出（print函数和input函数）
6. 控制结构
7. 条件语句（if, elif, else）
8. 循环结构（while循环，for循环）
9. 循环控制语句（break, continue）
10. 简单列表推导式
11. 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

1. 函数与模块
2. 函数定义与调用
3. 参数传递与返回值
4. 局部变量与全局变量
5. 匿名函数（lambda表达式）
6. 模块的使用（import语句）
7. 常用标准库模块（如math, datetime）
8. 面向对象编程
9. 类与对象的概念
10. 类的定义与对象的创建
11. 实例属性与方法
12. 类属性与类方法
13. 继承与多态
14. 特殊方法（如\_\_init\_\_, \_\_str\_\_等）
15. 异常处理
16. 异常的概念
17. try-except语句
18. 处理多种异常
19. finally子句
20. 自定义异常
21. 文件与输入输出
22. 文件的打开与关闭
23. 读取与写入文件
24. 文件上下文管理器（with语句）
25. 文件的其他操作（如删除、重命名）
26. 高级主题
27. 上下文管理器与with语句
28. 正则表达式和GREP语法
29. 数据科学相关库（如NumPy, Pandas）
30. 数据库管理与SQL
31. 数据库系统的基本概念
32. 数据库的分类和常见数据库软件
33. SQL 的特点
34. ★★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。
35. 查询多个列
36. 查询去重
37. SQL聚合函数
38. SQL 字符串函数
39. SQL数值函数
40. SQL⽇期和时间函数
41. SQL数据分组
42. ★★常见数据库的备份操作
43. ★★通过数据库日志恢复数据
44. ★常见数据库的客户端工具的使用
45. ★★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。
46. ★★数据库连接地址、连接口令的分析方法
47. ★数据结构与算法基础
48. 二叉树的定义及其主要特征
49. 二叉排序树
50. 赫夫曼（Hoffman）树和赫夫曼编码
51. 树和森林的遍历
52. 图的基本概念
53. 图的遍历算法
54. 普里姆算法和克鲁斯卡尔算法
55. 迪杰斯特拉算法
56. 弗洛伊德算法
57. 关键路径核心算法
58. 拓扑排序核心算法
59. 排序算法
60. 顺序查找算法
61. 折半查找算法
62. 二排序树的基本算法
63. B-树的基本概念和操作
64. B+树的基本概念和操作
65. 数据分析与挖掘的基础方法
66. ★★关键字搜索方法
67. GREP语法
68. 关键字的编码
69. ★★使用EXCEL或者WPS进行数据分析
70. 单元格格式调整方法
71. 数据查找和替换方法
72. 外部数据导入导出方法
73. 数据有效性检查方法
74. 日期和时间格式的处理方法
75. 数据筛选和排序
76. 数据分类汇总
77. 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
78. EXCEL两表数据比对方法
79. EXCEL常用统计公式使用
80. 日期函数：day，month，year，date，today，weekday，weeknum
81. 数学函数：product，rand，randbetween，round，sum，sumif，sumifs，sumproduct
82. 统计函数：large，small，max，min，median，mode，rank，count，countif，countifs，average，averageif
83. 查找和引用函数：choose，match，index，indirect，column，row，vlookup，hlookup，lookup，offset，getpivotdata
84. 文本函数：find，search，text，value，concatenate，left，right，mid，len
85. 逻辑函数：and，or，false，true，if，iferror
86. ★★文本编辑器数据处理
87. 列编辑模式的使用
88. 各类编码字符的搜索和替换
89. 正则搜索语法
90. ★★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

1. ★★网络安全基础
2. 流量分析识别网络安全威胁
3. 端口扫描与监听
4. 口令破解
5. 拒绝服务攻击
6. 漏洞攻击（缓冲区溢出、系统漏洞、应用软件漏洞）
7. 僵尸网络
8. 网络钓鱼
9. 网络欺骗
10. 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）
11. 使用Web编程语言发现和测试漏洞
12. 主流渗透测试和扫描工具的使用
13. 主流数据库语句以及SQL注入漏洞手工测试及绕过方法
14. 常见的漏洞原理和利用方式，会使用程序工具或技术方法检测。
15. 主流中间件和Web应用的常见安全隐患检测及加固方式
16. 恶意代码、文件传播方式判断和路径追溯
17. 通过Apache、IIS日志分析网络入侵行为
18. XSS漏洞手工测试方法
19. 利用系统日志、应用程序、安全日志等排查和溯源攻击行为。
20. 对内存数据进行分析，熟悉使用工具提取下列信息：
21. 进程信息，如进程名称、进程ID、线程信息等。
22. 网络连接，如IP地址、端口号、连接状态等。
23. 文件信息，如文件名、文件路径、文件大小等。
24. 注册表信息，如键值、权限设置等。
25. 系统信息，如操作系统版本、硬件配置等。
26. 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。
27. ★★逆向工程
28. 移动应用安全监测与防护
29. 熟悉Android、IOS调试、逆向工具使用，如apktool, jd-gui等安卓APK的反编译与加壳、动态调试技术、代码审计方法、移动应用的安全防护方法等。
30. 熟悉IOS ipa文件的反编译，动态调试。
31. IDA、WinDbg、OllyDbg、PEID等调试、逆向工具的使用。
32. 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。
33. ★加密与解密
34. 加密解密原理
35. Hash算法和数字签名原理
36. 对称与非对称加密算法原理
37. 字典穷举原理
38. 彩虹表原理
39. 常用的解密站点与工具
40. 加密文件的识别、查找方法
41. 常见“哈西+盐”的特征和识别方法
42. 常见文件加密工具的特点和识别方法
43. 常见磁盘加密的特点和识别方法
44. 密码破解技术及工具的使用方法
45. 暴力破解技术及工具
46. 基于数据字典破解技术
47. 基于社会工程学破解技术
48. 数据库密码破解
49. Windows的密码移除
50. 代码混淆加密与解密
51. asp混淆加密
52. php混淆加密
53. css/js混淆加密
54. VBScript.Encode混淆加密
55. ppencode
56. rrencode
57. jjencode/aaencode
58. JSfuck
59. jother

四、笔试题型样例

（一）单选题

《网络安全法》规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当符合哪些条件？

A. 关键信息基础设施的运营者在中国境内运营中收集和产生的重要数据和个人信息，只要经过所在国政府批准，即可向境外提供。

B. 关键信息基础设施的运营者在中国境内运营中收集和产生的重要数据和个人信息，必须经过网络安全审查办公室的审查通过，才可向境外提供。

C. 关键信息基础设施的运营者在中国境内运营中收集和产生的重要数据和个人信息，应当经过国家网信部门的安全评估，并经国务院有关部门同意后，才可向境外提供。

D. 关键信息基础设施的运营者在中国境内运营中收集和产生的重要数据和个人信息，应当经过国家网信部门的安全评估，并按照国家有关规定进行数据出境安全评估，才可向境外提供。

（二）多选题

下列哪些选项是常用的网络抓包工具？

A. Wireshark

B. Fiddler

C. Sniffer

D. Nping

E. tcpdump

（三）不定项选择题

在网络渗透过程中，攻击者通常会采取哪些手段来获取目标系统的敏感信息？

A. 扫描目标系统，寻找开放的端口和服务

B. 利用社会工程学手段，诱骗目标用户泄露信息

C. 使用恶意软件感染目标系统

D. 截获目标系统的网络通信数据

E. 对目标系统进行暴力破解攻击

（四）代码阅读题

阅读以下代码，并指出这段代码中存在哪些安全风险？请列举至少两处。

import socket

def create\_connection(host, port):

try:

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s.connect((host, port))

return s

except Exception as e:

print(f"Error: {e}")

return None

def send\_data(s, data):

try:

s.sendall(data.encode())

except Exception as e:

print(f"Error: {e}")

def receive\_data(s):

try:

data = s.recv(1024)

return data.decode()

except Exception as e:

print(f"Error: {e}")

return None

（五）简答题

1. 请简述网络渗透测试的步骤。

2. 请描述一种常见的对称加密算法的工作原理，并解释其安全性基础。

3. 请根据下面的示例简述解释HTTP请求和响应的基本结构。

GET /index.html HTTP/1.1

Host: www.example.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK

Content-Type: text/html; charset=UTF-8

Set-Cookie: session=123456789; path=/

Cache-Control: no-cache, no-store, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Expires: 0

Content-Length: 12345

五、机试题型样例

（一）网络攻击测试

对给定的靶机（虚拟机）开展网络攻击测试，找到靶机中隐藏的若干flag并回答问题。

1. 靶机开放端口有哪些？
2. 靶机对外发布的网站业务名称和版本是什么？
3. 针对靶机存在的漏洞拿到该网站服务器的webshell权限，找到flag1。
4. 找到服务器后台数据库的配置文件中的flag2，并列出数据库的用户名和密码。
5. 网站后台管理员的密码是什么？
6. 服务器用户flag3的密码是什么？
7. 用户flag4的登录次数有多少次，请列出具体时间。
8. apk文件的逆向分析

对给定的apk文件进行分析，按要求回答问题。

1. 截图展示apk文件运行后的界面，并展示该apk运行后需要申请哪些权限，请列出。
2. 该apk文件的软件包名称是什么？
3. 该apk文件校验注册授权使用的加密算法是哪个？
4. 静态分析 so代码，确定flag1的值长度为多少位？
5. 编写解密脚本，完成对图片的解密。