附件3

2025年度广西壮族自治区公安机关

网络安全职位专业笔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2025年度公安机关网络安全职位专业笔试和专业技能测试，特制定本大纲。

一、考试性质和目标

网络安全职位专业笔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网络安全专业基础知识、专业技能素养以及解决实际问题的能力。

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

**（一）考试方式**

**专业理论测试**采用闭卷笔试考试方式，题目分为单项选择题、多项选择题和判断题三种类型。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。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。

**（二）作答要求**

**专业理论测试**报考人员务必携带的考试文具包括黑色字迹的钢笔或签字笔、2B铅笔和橡皮，在指定位置上填写准考证号、姓名等信息，并在答题卡上用2B作答，在试题本或其他位置作答一律无效。

**专业技能测试**实机操作过程、结果必须填写到电子答卷上，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。交卷时需将电子答卷及附件文件压缩为1个文件，并计算压缩文件的哈希校验值。

三、考试内容

专业笔试和技能测试的考察内容包括计算机、软件、网络安全、信息安全、大数据、人工智能等方面。

第一编 法律法规基础知识

1. 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.最高人民法院、最高人民检察院、公安部《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）《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》（法发〔2016〕22号）

5.公安部《公安机关办理刑事案件电子数据取证规则》

第二编 专业基础知识

1. 计算机基础

1.计算机组成原理

2.操作系统基础

3.数据结构基础

4.C/C++、Java、Python等程序设计基础

1. 计算机网络

1.计算机网络体系结构与参考模型

2.常见网络协议及其应用

3.常见网络设备使用与配置

1. 大数据技术基础

1.容器集群的管理

2.分布式文件系统

3.图数据库

1. 人工智能基础

1.机器学习算法

2.深度学习

1. 密码学基础

1.加密解密原理

2.加密文件的识别、查找方法

1. 操作系统安全基础

1.Windows操作系统安全

2.Linux操作系统安全

3.MacOS操作系统安全

4.移动操作系统安全

第三编 网络安全实操能力

1. 操作系统安全检测与防护

1.熟悉Windows、Linux等常见操作系统的常规安全防护技术，利用系统日志、应用程序日志等排查和溯源攻击行为；

2.操作系统用户、文件系统、网络、服务等安全检测和加固方法。

1. 数据库安全检测与防护

1.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；

2.数据库SQL注入漏洞手工测试方法，入侵防护、访问控制、身份认证、数据加密等安全措施；

3.数据库的客户端程序管理、应用系统访问和重要操作审计等技术实现。

1. Web应用安全检测与防护

1.常见Web应用环境搭建、运维和重建技术；

2.常见Web编程语言；

3.中间件和Web应用的安全检测与防护方法；

4.使用程序工具或技术方法检测并修复常见的Web漏洞。

1. 恶意程序（代码）分析
2. 熟悉恶意程序（代码）的识别方法及防护措施，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；
3. 能对常见恶意程序（代码）进行混淆还原和逆向分析。
4. 移动应用安全检测与防护
5. 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；
6. 熟悉移动应用的安全防护方法。
7. 电子数据取证分析
8. 进行逻辑数据恢复和电子数据完整性校验；
9. 对常见操作系统和网站、数据库、FTP、邮件等服务器日志进行分析；
10. 对操作系统、网络、进程、服务、用户、注册表、文件和历史记录等信息进行搜集和痕迹分析；
11. 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。
12. 大数据分析
13. 熟悉文本字符、网络流量、系统日志、访问记录等数据的分析方法，使用GREP语法查询数据；
14. 运用相关工具或者编写程序实现数据清洗、数据分析和数据加解密工作。

四、笔试题型样例

（一）单选题

1. 《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。

2. 在Web应用中，如果开发者未对用户输入进行适当处理，可能导致哪种漏洞？ （ ）

A. DDoS攻击

B. CSRF漏洞

C. 反射型XSS

D. 缓冲区溢出

3. 在Web开发中，哪种措施可以有效防止会话劫持？（ ）

A. 使用HTTPS

B. 禁用JavaScript

C. 限制用户登录次数

D. 对用户输入进行转义

3. 在Linux系统中，存储用户登录记录（包括登录、登出及非法访问等记录）的文件是哪个？ （ ）

A. /var/log/messages

B. /var/log/lastlog

C. /var/log/auth.log

D. /var/log/user.log

（二）多选题

1.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

2.在MySQL中，为了加强数据库安全性，防止未授权访问和恶意操作，以下哪项配置不能限制一个用户的权限。（ ）

提示：仅允许其在特定数据库上执行SELECT和INSERT操作，同时防止用户执行其他敏感操作，如DROP和UPDATE。

1. 使用GRANT SELECT, INSERT ON <database>.\* TO '<user>'@'<host>' IDENTIFIED BY '<password>'，并且在REVOKE命令中禁止其他权限
2. 配置read\_only=ON，限制所有用户仅能执行SELECT操作，阻止对数据的修改
3. 配置skip\_grant\_tables，绕过权限系统直接操作数据库
4. 使用GRANT SELECT, INSERT ON <database>.\* TO '<user>'@'<host>'，并且在FLUSH PRIVILEGES后删除不必要的用户

3.下列哪些属于安卓应用程序的常见加固方式？（ ）

A.动态加载DEX

B.APK包外AES加密

C.VMP代码混淆

D.so section加密

E.DEX整体加密

（三）判断题

1. 设置Content Security Policy（CSP）措施可以有效防止点击劫持攻击。 （ ）

2. 防止SQL注入的最佳实践是使用预编译语句（prepared statements）或参数化查询。 （ ）

五、机试题型样例

（一）网络攻击测试

1. 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。

2.对给定的靶机（虚拟机）开展网络渗透测试，找到相应flag。靶场环境及答案参考：https://developer.aliyun.com/article/1221168

（二）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。

（三）电子数据取证

查找2024年该服务器最后一次远程登陆的时间？（提交形式如: 2021-09-30-12:30:05）

操作提示：远程登录的事件号是4648。

（四）移动应用的安全检测

对于给定的检材1，请指出该应用程序判断用户是否开通永久VIP？具体是如何实现的（附代码进行说明）？请修改这些代码，将该应用程序破解成为永久VIP版本（说明过程并附破解成功后的运行图）。

操作提示：

1. 使用jadx对“懒人驾考”APK进行反编译。分析逆向后的Java代码，发现该APK中关于永久VIP的关键字符串是key\_mmkv\_vip\_list\_forever。
2. 在jadx中使用全局搜索，发现该字符串位于com.jx885.lrjk.c.b、com.jx885.lrjk.c.c、com.jx885.lrjk.cg.ui.activity处有casewhen、if等条件判断方法。
3. 修改代码，将判断开通永久VIP为真就开启VIP入口点的判断条件改为永真。
4. 方法不唯一，可以定义值为true的局部变量并传参给if，或者将原有的b.G(1)传参修改为b.G(1) or b.G(0)等等。