江苏省2022年度公安机关网络安全技术（网络安全防护）特殊专技职位专业笔试和技能测试大纲

为便于报考者充分了解江苏省2022年度公安机关网络安全技术（网络安全防护）特殊专技职位专业笔试和技能测试，特制定本大纲。

一、测试方式

江苏省2022年度公安机关网络安全技术（网络安全防护）特殊专技职位专业笔试采用闭卷考试方式，考试时限120分钟，满分100分。技能测试采用现场实操方式，考试时限120分钟，满分100分。

二、作答要求

报考者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。专业笔试报考者在指定位置上填写准考证号、姓名等信息，并在指定位置上作答，在试题本或其他位置作答一律无效。技能测试报考者按照测试要求，在测试系统中提交正确答案和解题过程。

三、测试内容

江苏省2022年度公安机关网络安全技术（网络安全防护）特殊专技职位专业笔试、技能测试，主要测查岗位所需的专业基础知识、专业技能素养以及解决问题的实际能力，包括网络安全法

律规范、理论基础知识、网络安全防护实践能力等方面。

（一）网络安全法律规范。主要测查报考者掌握《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《最高人民法院、最高人民检察院、公安部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）相关内容的能力。

（二）理论基础知识。主要测查报考者掌握网络安全理论基础知识，及运用相关知识分析与解决问题的能力。

1.计算机基础知识

（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

2.计算机网络基础

（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

3.密码学基础

（1）分组密码学原理与应用

（2）公钥密码学原理与应用

4.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

5.数据库安全基础

（1）常见数据库命令与SQL语言基础

（2）数据备份与还原

（3）关系型数据库安全

（4）非关系型数据库安全

6.WEB应用安全基础

（1）Web应用安全配置

（2）Web前后端开发基础

（3）常见Web漏洞原理与检测

（4）中间件安全基础

7.二进制安全基础

（1）程序逆向分析

（2）漏洞分析与检测

（3）常见病毒木马技术原理

（三）网络安全防护实践能力。主要测查报考者利用相关程序工具和技术方法开展网络安全防护的实践能力。

1.操作系统安全检测与防护

了解Windows、Linux等常见操作系统的常规安全防护技术。能熟练利用系统日志、应用程序日志等排查和溯源攻击行为；掌握对系统用户、文件系统、网络、服务等安全检测和加固方法。

2.数据库安全检测与防护

了解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。熟悉数据库入侵防护、访问控制、身份认证、数据加密等安全措施；深入了解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。

3.Web应用安全检测与防护

了解常见Web应用环境搭建、运维和还原技术；熟悉常见Web编程语言；掌握中间件和Web应用的安全检测与防护方法。能够使用程序工具或技术方法检测并修复常见的Web漏洞。

4.恶意程序（代码）分析

熟悉恶意程序（代码）的识别方法及防护措施。能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。

5.移动应用安全检测与防护

了解移动智能终端操作系统、移动应用软件的常规安全漏洞检测和防护技术。熟悉移动应用的逆向分析和代码审计技术、移动应用的安全防护方法等。

6.电子数据取证分析

了解常见的电子数据取证技术和分析方法。能运用相关工具进行逻辑数据恢复和电子数据完整性校验，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，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，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。

7.数据分析处理

了解文本字符、网络流量、系统日志、访问记录等形式数据的分析方法。能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、题型介绍

专业笔试部分设单项选择题、多项选择题和判断题等3种题型。技能测试部分考察技术实践能力，考试系统提供常用软件工具，考生按照技能测试题目要求，通过技术方法获取正确答案。不同考生之间的网络环境相互独立，网络采用局域网方式，禁止访问互联网。