

**第六届连云港技能状元大赛
网络与信息安全管理项目技术工作文件**

2025 年 9 月

为保证连云港市网络和数据安全技能竞赛顺利进行，现将本次竞赛有关技术文件内容说明如下，请参照执行。

一、竞赛职业

网络和信息安全管理员

二、竞赛标准

竞赛参照《网络与信息安全管理员国家职业标准》（三级/高级工）及以上要求命制竞赛试题，根据《网络安全法》《数据安全法》《个人信息保护法》等相关法律法规要求，重点是网络安全知识掌握与综合运用，网络安全攻防实战技能，网络安全实际问题解决等方面的竞赛。比赛内容结合行业实际，适当增加新知识、新技术、新理念等相关内容，包括但不限于网络安全等级保护、相关法律法规等理论知识以及技能操作知识（WEB 安全、病毒分析与处置、代码审计、逆向工程、漏洞利用、加密算法、应急响应、取证分析等操作技能）。

三、选手自备材料

参赛选手需自备性能稳定、可正常使用的笔记本电脑，并确保设备具备良好的网络和硬件兼容性。选手应自行准备有线网络接口设备（RJ45 网口转换器或网卡）、有线鼠标等必要外设，以保证竞赛过程中操作的稳定性和连续性。

同时，选手需提前安装和配置常用的网络与安全分析工具及软件环境，包括但不限于：虚拟化软件（如 VMware Workstation/VMware Fusion）、Web 渗透测试工具（如 Burp Suite）、网络扫描与探测工具（如 Nmap）、网络抓包与协议分析工具、日志分析工具、杂项分析工具、密码学工具、Python 运行环境及常见第三方库文件等。

选手可根据个人习惯及赛事需求，额外准备其他辅助工具和软件，确保竞赛中能够高效完成相关操作与任务。

四、竞赛内容

竞赛决赛采用线下部署竞赛平台方式进行，竞赛内容：包括理论知识和技能比赛两部分，两部分各单项总分为 100 分。总成绩计算：理论知识竞赛成绩占总成绩 20%，技能比赛成绩占总成绩 80%，两项成绩合计为总成绩（保留小数两位），从高分到低分排名，整体时长 180 分钟。

（一）理论知识赛考试采用上机考试进行，时间为 60 分钟，考试题型分为单项选择题、多项选择题、判断题三种，试题总分为 100 分，考查网络安全基础知识、数据安全理论、信息安全法律法规及安全管理体系等，选手需在规定时间内完成操作并提交结果。

题型	题量	分值
单项选择题	60 题(每题 1 分)	60
判断题	10 题(每题 1 分)	10
多项选择题	15 题(每题 2 分)	30
合计		100

（二）技能操作竞赛采取上机考试形式进行，时间为 120 分钟，试题总分为 100 分，比赛中对选手的技能要求主要包括：API 接口安全、数据注入、数据高频采集、数据加解密、敏感数据识别、数据分类分级、数据脱敏、逆向分析、数据溯源与处置、模型数据安全、人工智能安全等。

1. CTF 实操题（5 题）：将业务场景抽象成对应技术点和应用的赛题，并通过预置答案的方式来验证选手是否可以分析场景发现漏洞。

2. 数据分析题（2 题）：模拟仿真相关数据安全事件，提供选手对应事件的流量报文、系统日志、磁盘镜像等文件。选手通过分析相关的事件和文件内容进行解题。

3. 人工智能安全题（1 题）：主要考核对人工智能安全相关解题能力。选手通过分析场景描述及要求完成解题，通过上传指定附件格式至平台完成解题，解题过程限次提交次数。

五、竞赛专业技术纲要

（一）理论知识

政策法规与标准。熟悉《网络安全法》、《数据安全法》、《密码法》、《个人信息保护法》，理解法律责任与义务。了解《国家网络安全事件应急预案》及网络安全应急响应流程。掌握 ISO/IEC 27001 等国际标准及《信息系统安全等级保护实施指南》、GB/T 43697 等国内数据安全标准。

（二）技能操作

1. 风险评估

熟悉渗透测试技术与工具（如 Metasploit、Kali Linux），掌握漏洞分析与修复。

了解数据安全风险评估标准与技术，能进行数据安全分析。

2. 系统安全管理

管理用户权限与文件夹访问权限，定期更新系统补丁。

使用日志审计与分析工具进行安全监控。

3. 数据安全

应用数据分类分级标准，掌握数据脱敏、加密与恢复技术。
熟悉数据销毁技术，确保敏感数据的完全销毁。

4. 物联网安全

分析物联网设备固件与协议，掌握二进制逆向技术（如 ARM、MIPS 架构）。

5. 应急响应与取证

使用入侵检测与取证工具（如 Kali Linux、Volatility），进行系统攻击溯源与事件响应。

加固系统安全配置，强化用户权限与文件系统安全。

6. 人工智能安全

了解 AI 安全风险与防护技术，确保训练数据与模型的安全性。

防范对抗性攻击与数据泄露，确保 AI 系统的可靠性。

7. 恶意代码分析与防护

识别并隔离恶意代码，运用动态分析与逆向技术进行分析。

8. 其他安全技术

掌握密码学基本原理，常见加密算法与协议（AES、RSA 等）。

熟悉移动恶意程序分析与防护，使用 Wireshark 等工具进行网络协议分析。

精通数据恢复技术与恶意代码防护，了解量子密码学和区块链的基本安全技术。

竞赛内容与时间安排

序号	名称	时间	单项 分值	权重	方式
----	----	----	----------	----	----

1	理论知识	60 分钟	100	20%	机考
2	技能操作	120 分钟	100	80%	机考

六、设备设施要求

赛场提供设施、设备清单表

序号	名称	数量	技术规格
1	交换机	3 台	2 台 48 口二层交换机、1 台 24 口三层交换机。
2	网络安全竞赛平台	2 个	支持理论赛、解题赛、攻防赛常见形式，不局限于单一形式，同一场竞赛各形式之间可随意组合。

七、比赛要求

1. 线下赛参赛选手须提前 30 分钟入场，利用现场条件测试网络连通性及竞赛系统账号和口令；裁判长宣布比赛开始后后方可作答。

2. 比赛正式开始 30 分钟后不得进入赛场，比赛结束前选手不得离开比赛区域，比赛过程中所有问题请先举手示意，不得擅自离开座位，去洗手间由工作人员陪同。

3. 参赛选手须自带稳定可用的笔记本电脑（仅限一台）参加竞赛，并自行配置有线网口和有线鼠标，若出现因自带电脑原因无法连接竞赛系统的情况，责任自负。

4. 参赛选手禁止携带手机等与比赛无关的具有通信功能电子设备（包括但不限于智能手表、手环、蓝牙耳机、智能眼镜、网盘等）、U 盘、硬盘等物品进入赛场，禁止携带网络安全类硬

件设备进入赛场，手机等各种电子设备在进入赛场前统一存放在存包柜，违规者立刻取消比赛资格。

5. 竞赛过程中，禁止使用 DDOS 工具攻击竞赛系统和考题系统；禁止根据渗透得到的权限进行特权数据的更改，对赛事环境造成影响；禁止利用扫描器对竞赛系统和考题系统进行恶意探测扫描。

6. 参赛选手除完成竞赛考题要求外，严禁各种攻击行为。一经发现攻击行为，立即取消参赛资格。

7. 竞赛进行期间，参赛选手须填写网络配置确认单进行网络责任归属，由于选手原因造成的网络损坏，选手须承担后果。

8. 竞赛进行期间，竞赛场地内将开启信号干扰器、信号屏蔽器等设备，屏蔽现场的手机信号和无线网等。

9. 参赛选手须服从大赛工作人员的管理，接受监考人员的监督和检查，一经发现参赛选手出现违反竞赛纪律的行为，立即取消参赛资格，情节严重者将通报批评。

八、竞赛成绩

线下决赛竞赛总成绩=理论赛得分+实操闯关赛得分。依据总成绩高低排出个人名次，当总成绩相同时，以实际操作成绩高者为先。

九、裁判机构与原则

比赛裁判工作遵循公平、公正、公开的原则。本赛项的裁判组成员由本届竞赛裁判委员会组建。

十、说明

连云港市网络与信息安全管理项目文件一切解释权归竞赛

主办单位所有。

十一、样题

（一）理论赛

【单选题】以下哪一项不是我国与信息安全有关的国家法律。

- A. 《信息安全等级保护管理办法》
- B. 《中华人民共和国保守国家秘密法》
- C. 《中华人民共和国刑法》
- D. 《中华人民共和国国家安全法》

答案：C

1. 【多选题】Linux 关机命令包括（）。

- A. halt
- B. shutdown -h now
- C. poweroff
- D. init 0

答案：ABCD

2. 【判断题】对抗样本攻击仅对计算机视觉模型有效，不影响自然语言处理模型。

答案：错误

解析：对抗样本可攻击任何类型的 AI 模型，包括 NLP 和语音模型。

（二）实操闯关赛

1. CTF 实操题

题目名称：KeyReceiver

题目难度：中

题目描述：某公司一员工由于存储不当导致一个密钥文件损坏，无法解密相关重要文件。安全部门的小 A 通过技术手段恢复了部分密钥文件数据，请你帮助小 A 完整恢复密钥文件，并尝试解密获得 flag。

答案：flag{0247920a5eeb9c3db026e9e9dbbf6a27}

附件名：task.zip

2. 数据分析题

【场景描述】

某公司下属分支机构业务部门的一位同事，将一些较为敏感的数据传输给公司总部进行汇总分析，该同事将敏感数据拆分成了两份，并使用不同方式进行传输。现总部数据安全负责人怀疑有数据泄露的风险，截获数据包进行分析，请参赛选手协助该公司数据安全负责人，分析他截获的数据包，分析是否存在潜在问题或风险。

【场景题干】

1. 请根据给定的明文网络流量数据包，利用适当的工具和技术，准确获取明文传输过程中传输的明文数据的数量。将获取的明文数据的数据量作为答案提交。

【评测标准】本题按结果给分。最终提交结果为(flag{数量})，若敏感数据量为 1000，即提交：flag{1000}。

2. 请根据给定的密文数据包，利用适当的工具和技术，准确解密其中的明文数据，并将解密获取的第 100 条明文数据作为答案提交。

【评测标准】本题按结果给分。最终提交结果为(flag{md5(明

文数据})), 若明文数据为: 姓名_手机号_岗位_地址, 即提交:
flag{md5(姓名_手机号_岗位_地址)}。

3. 模型安全题

【背景】

随着大数据和 AI 技术快速发展, 数据质量与安全预处理是保障在线团购商城稳定运行和决策效果的关键。平台依赖用户和商品数据进行精准营销、个性化推荐和风险控制, 但原始数据可能存在缺失、异常、错误或恶意内容, 直接影响分析和模型训练。不安全的预处理流程可能导致数据泄露、隐私侵犯和系统漏洞。提升数据预处理安全性对平台发展和用户权益至关重要。

【场景描述】

您作为一家在线团购商城的安全工程师, 负责评估和提升平台数据预处理流程的安全性。平台需要对用户评论、商品信息等数据进行清洗、标注、转换等预处理操作, 为后续的推荐系统和风控模型提供高质量的数据支撑。本次竞赛, 您将模拟真实的数据预处理场景, 深入研究数据清洗、特征工程、数据标注、数据完整性校验、数据脱敏、恶意代码检测等关键安全环节, 旨在全面检验和提升在线团购商城数据预处理的安全防线, 并为构建安全可靠的数据预处理流程提供技术方案。

任务一: 数据标注与完整性校验

【题干描述】

针对在线团购平台提供的原始用户评论数据, 爬取用户评论数据, 进行情感标注(正面/负面), 并基于用户 ID、用户名、手机号生成 MD5 签名以校验完整性。按附件模板和任务书要求提

交处理后的 submit_1.csv 文件进行评分。

【平台提供】

Web 环境: 一个模拟在线团购商城数据平台, 提供用户评论、商品信息等原始数据浏览功能。

附件: 任务一答案提交模板.csv (包含字段: user_id, label, signature)