

江西省第二届职业技能大赛

“网络安全”项目技术工作文件

(世赛选拔)

2025 年 3 月

# 目 录

1.项目简介 .....	1
1.1 项目描述 .....	1
1.2 考核目的 .....	1
1.3 相关文件 .....	1
2.基本能力与职业标准 .....	2
3.竞赛内容 .....	7
3.1 考核内容 .....	7
3.2 竞赛模块 .....	7
3.3 模块简述 .....	8
3.3.1 模块 A: 网络安全事件响应 .....	8
3.3.2 模块 B1: 漏洞评估与修复 .....	8
3.3.3 模块 B2: 网络安全攻防 .....	8
3.4 命题方式 .....	8
3.5 竞赛日程及地点安排 .....	9
4.评分标准 .....	12
4.1 评价分（主观） .....	12
4.2 测量分（客观） .....	12
4.3 评分流程说明 .....	12
4.4 统分方法 .....	13
4.5 裁判构成和分组 .....	13
5.竞赛相关设施设备 .....	15

5.1 场地设备 .....	15
5.2 材料（软件） .....	16
5.3 竞赛选手自备的设备和工具 .....	17
5.4 竞赛场地禁止自带使用的设备和材料 .....	17
6. 项目特别规定 .....	18
7.赛场布局要求 .....	19
8.健康安全和绿色环保 .....	19
9.开放赛场 .....	20

本项目技术工作文件（技术描述）是对本竞赛项目内容的框架性描述，正式比赛内容及要求以竞赛最终公布的赛题为准。

## **1.项目简介**

### **1.1 项目描述**

网络安全项目旨在考察选手保护企业信息系统的的能力，防止黑客入侵和窃取敏感数据。选手需要配置防火墙、入侵检测系统、服务器等网络安全设备，并制定网站安全解决方案，确保企业系统的安全。同时，他们还需维护和实施网络安全监控策略，调查并响应企业内部的网络安全事件。选手需要进行安全渗透测试，提前发现并修补可能被黑客利用的漏洞，以加强系统的安全防护。此外，竞赛还涉及虚拟化基础设施安全管理，要求选手通过代码审计、用户流量分析、渗透测试等技术手段，保障企业关键数据的安全性，防止数据泄露、篡改或破坏。

该项目对应的职业（工种）：网络与信息安全管理员（4-04-04-02）。

### **1.2 考核目的**

本项目旨在全面评估选手在网络安全领域的技术能力和综合素质。选手需要掌握攻击者常用的渗透技术及最新安全防护手段，确保企业信息系统能够有效抵御各类网络攻击。此外，选手须具备数字取证能力，能够收集、分析和处理与网络安全事件相关的证据，协助执法机构打击网络犯罪和防范网络欺诈。除了技术能力，竞赛还考核选手的表达、书写、沟通和协调能力，要求他们具备较强的综合素质，以应对快速发展的网络安全挑战。

### **1.3 相关文件**

本项目技术工作文件只包含项目技术工作的相关信息。除阅读本文件外，开展本技能项目竞赛还需配合其他相关文

件一同使用：

竞赛样题 - 提供参考题目，帮助选手熟悉竞赛题型和考核内容。

设备与工具使用说明 - 介绍竞赛所用设备、软件及工具的使用方法和注意事项。

## 2.基本能力与职业标准

选手基本知识与能力要求表：

相关要求		权重比例 (%)
1	工作组织和管理	5
基本知识	选手需要了解和理解： 健康与安全相关的法规、义务、规定和文档 必须使用个人防护用品的场合，如：静电防护 在处理客户设备和信息时的完整性和安全性 废物回收、安全处置的重要性 计划、调度和优先处置的方法 在所有的工作过程中，准确、检查和注意细节的重要性 系统性开展工作的重要性	
工作能力	选手应具备的能力： 遵守健康和安全标准、规则和规章制度 保持安全的工作环境 识别并使用适当的个人静电防护设备 安全、妥善地选择、使用、清洁、维护和储存工具和设备 规划工作区域，最大化工作效率，并维持日常整洁的相关规定 有效地工作，并定期检查进度和结果 保持与职业岗位要求一致的技能水平 采取全面有效的研究方法，确保知识不断更新 为客户提供设备的使用和可持续性的规划 积极尝试新方法、新制度，拥抱变革 能够安全的和可持续地处置电子数据存储设备	
2	沟通和人际交往	
基本知识	选手需要了解和理解： 倾听作为有效沟通一部分的重要性 同事的角色和同事的需求，和最有效的沟通方式	10

	<p>与同事和经理建立富有成效的工作关系的重要性</p> <p>有效的团队合作技巧</p> <p>消除误会和化解冲突的技巧</p> <p>管理紧张和愤怒情绪以解决面临的困难情况</p> <p>网络安全调查的过程需要有完整的文档记录</p>	
工作能力	<p>选手应具备的能力:</p> <p>加强倾听和提问技巧, 加深对复杂情况的理解</p> <p>保持有效的队友之间的口头和书面沟通</p> <p>识别和适应队友变化的需求</p> <p>为发展强大而高效率的团队作出积极贡献</p> <p>与队友分享知识和专业技能, 发展出相互支持的学习文化</p> <p>管理好紧张/愤怒等情绪, 遇到问题能有解决有信心</p> <p>调查过程中准确地记录步骤和发现结果</p> <p>确保所有安全和信息系统操作方面的政策和工作流程都被严格遵守</p>	
3	安全系统的设计和建设	
基本知识	<p>选手需要了解和理解:</p> <p>IT 风险管理标准, 策略, 要求和程序</p> <p>网络安全防护和脆弱性的检测工具及其功能</p> <p>操作系统</p> <p>网络系统</p> <p>计算机编程概念, 包括计算机语言、编程、测试、调试和计算机文件类型</p> <p>软件开发的网络安全、隐私保护的原则和方法</p>	
工作能力	<p>选手应具备的能力:</p> <p>在设计和记录总体程序测试和评估过程时, 应将网络安全和隐私原则应用于组织要求 (与保密性、完整性、可用性、可控性、不可否认性相关)</p> <p>独立进行综合测试, 包括管理、运行和技术安全控制、信息系统内部或者源自信息系统的增强控制功能等, 判断、决定整体控制效果</p> <p>开发、使用网络安全评估系统, 以评估相关系统符合规范和要求</p> <p>确保合并 IT 系统元素的安全性和系统的互操作性</p> <p>修改现有的计算机应用程序、软件或专门应用程序</p> <p>分析新的或者现有计算机应用程序、软件的安全状况, 提供准确可靠的分析报告</p> <p>开发和维护业务、系统和信息流程以支持企业任务需求</p> <p>开发描述基线和信息系统体系结构的技术规则和要求</p> <p>确保利益相关各方安全需求, 保护企业运营和商业流程在企业架构的各个方面得到正常处理, 包括参考模型、部分和解决方案架构、确保系统支持企业的运营和商业</p>	10

	<p>流程</p> <p>对系统工程和软件系统进行安全研究，开发相应的安全功能，并将其部署到系统中</p> <p>开展研究（包括渗透测试）来评估网络空间系统中潜在的脆弱性</p> <p>咨询相关人员，评估功能需求，并将功能需求转换为技术解决方案</p> <p>计划、准备和实施系统测试</p> <p>根据技术规范和要求，进行分析、评估并报告结果</p> <p>设计、开发、测试和评估信息系统的安全情况，涵盖系统开发生命周期</p>	
4	系统安全运维	
基本知识	<p>选手需要了解和理解：</p> <p>查询语言，如结构化查询语言、数据库系统等</p> <p>网络协议，如 TCP/IP、动态主机配置、DNS 和目录服务等</p> <p>防火墙概念和功能（如单点身份验证、审核、策略执行，恶意内容的邮件扫描，遵从性数据匿名化，数据丢失保护扫描，加速加密操作，SSL 安全，REST、JSON 处理等）</p> <p>网络安全体系结构的概念，包括拓扑、协议、组件和原则</p> <p>系统管理、网络和操作系统加固技术</p> <p>组织信息技术用户安全策略（如帐户创建、密码规则、访问控制等）</p> <p>信息技术安全原则和方法</p> <p>身份验证、授权和访问控制方法</p> <p>网络安全、漏洞和隐私原则</p>	15
工作能力	<p>选手应具备的能力：</p> <p>安装、配置、测试、操作、维护、管理网络体系架构</p> <p>管理好分享和传输所有数据的软件</p> <p>安装、配置、调试和维护服务器（硬件和软件），确保信息保密性、完整性和可用性</p> <p>系统密码、账户的创建和管理，并实施相应的访问控制策略</p> <p>分析机构当前的计算机系统，设计信息系统解决方案，以帮助机构更安全、高效和有效地运行</p> <p>开发监视和测量风险、合规性和保证工作的方法</p> <p>对信息系统、基础设施网络进行审计，以提供持续优化、网络安全和解决问题的支持</p>	
5	安全系统的保护和防卫	
基本知识	<p>选手需要了解和理解：</p> <p>文件系统</p>	15

	<p>系统文件（如日志文件、注册表文件、配置文件等） 包含相关信息以及在何处查找这些系统文件</p> <p>网络安全体系结构的概念，包括拓扑、协议、组件和原则（如纵深防御的应用）</p> <p>行业标准和组织性接受的分析原则、方法和工具来识别漏洞</p> <p>威胁调查、报告，调查工具和法律、条例</p> <p>事件类别、响应和处理方法</p> <p>网络防御和漏洞评估工具及其功能</p> <p>对于已知的安全风险的应对措施设计</p> <p>身份验证、授权和访问方法（如基于角色的访问控制、强制访问控制和任意访问控制等）</p>	
工作能力	<p>选手应具备的能力：</p> <p>使用防护措施和不同渠道收集的信息，以识别、分析和报告发生的或可能发生的网络事件，以保护信息、信息系统和网络免于威胁</p> <p>测试、实施、部署、维护、检查、管理硬件基础架构和软件，按要求有效管理的计算机网络防护服务提供商的网络和资源</p> <p>监视网络，及时修订未授权的活动</p> <p>在所属的领域对危机或者紧急状态做出有效响应，在自己的专业领域中降低直接的和潜在的威胁</p> <p>使用缓解措施、准备措施，按照要求做出响应和实施恢复步骤，以最大化存活率，保存财产和信息的安全</p> <p>调查和分析所有的相关响应活动</p> <p>对威胁和漏洞进行评估</p> <p>确定与可接受的配置、企业或本地策略的偏差</p> <p>评估风险水平，制定或建议在业务和非运营情况下采取适当的缓解措施</p> <p>根据记录好的企业工作流程开展安全事件的灾备和恢复</p>	
6	操作和管理	
基本知识	<p>选手需要了解和理解：</p> <p>网络威胁行为和他们的方法</p> <p>用于检测各种可利用的活动的技术和方法</p> <p>网络情报和信息收集能力</p> <p>网络威胁和漏洞</p> <p>网络安全基础知识（如加密、防火墙、认证、诱捕系统、外围保护等）</p> <p>漏洞信息传播源（如警报、通知、勘误表和公告等）</p> <p>哪些系统文件（如日志文件、注册表文件、配置文件）包含相关信息以及在何处查找这些系统文件</p> <p>开发工具的结构、方法和策略（如嗅探、记录键盘等）</p> <p>和技术（如获取后门访问、收集机密数据、对网络中的其他系统进行漏洞分析等）</p>	20



	<p>预测、模拟威胁能力和行动的內部策略</p> <p>内部和外部合作伙伴的网络操作能力和工具使用能力</p> <p>目标开发（如概念、角色、责任、产品等）</p> <p>系统开发过程遗留物和司法鉴定应用案例</p> <p>应用于现有已安装系统和软件的新兴网络攻击和网络威胁</p> <p>为防止自然灾害进行灾备的重要性</p>	
工作能力	<p>选手应具备的能力：</p> <p>识别和评估网络安全罪犯或外国情报机构的能力和活動</p> <p>提供调查结果，来帮助法律程序和反间谍调查（或反间谍活动）的启动，或支持法律程序和反间谍调查（或反间谍活动）的执行</p> <p>分析搜集到的信息，找到系统弱点和潜在可被利用的环节</p> <p>分析来自情报界的不同渠道、不同学科和不同机构的威胁信息</p> <p>根据背景情况，同步和放置情报信息，找出可能的影响</p> <p>应用来自一个或多个不同地区、国家、非政府机构和技术领域的最新知识</p> <p>应用语言、文化和专业技术知识，进行信息收集、分析和其他网络安全活动</p> <p>识别、保存和使用系统开发过程遗留物并用于分析数据丢失时，成功执行数据和系统恢复</p>	
7	情报收集与操作	
基本知识	<p>选手需要了解和理解：</p> <p>收集策略、技术和工具</p> <p>网络情报获取和信息收集能力</p> <p>信息需求和收集要求在扩展的企业中被翻译、跟踪和优先处理</p> <p>需要与网络运营规划相关的智能规划产品</p> <p>网络运营规划计划、战略和资源</p> <p>网络操作策略、资源和工具</p> <p>网络操作概念、术语、词汇（如环境准备、网络攻击、网络防御等）、原则、能力、限制和效果</p>	10
工作能力	<p>选手应具备的能力：</p> <p>使用适当的策略，创建的优先级别，通过收集管理过程进行数据收集</p> <p>执行深入的联合目标确定和网络安全规划流程</p> <p>收集信息并制定详细的运营计划和订单支持要求</p> <p>协助综合信息和网络空间作战的全方位作战的战略和作战层面规划</p> <p>支持收集有关犯罪或外国情报实体的证据的活动，以减轻可能或实时的威胁，防止间谍或内部威胁、外国破坏、</p>	

	国际恐怖活动，或支持其他情报活动	
8	调查和电子取证	
基本知识	选手需要了解和理解： 威胁调查、报告、调查工具和法律 恶意软件分析的概念和方法 收集、打包、传输和储存电子证据的过程，同时维持监管链 持久性数据的类型和集合 数字取证数据处理的概念和实践 数字取证数据的类型和识别方法 操作系统结构和操作对于取证的意义 网络安全漏洞的具体操作性影响	15
工作能力	选手应具备的能力： 通过日志和其他信息源跟踪重要信息，以确定构成事件的事件链 识别可能发生攻击的过程，以便能够评估事件以及基础设施可能受到影响的方式 推断事件中采取的步骤，以识别系统中存在的任何弱点 仔细关注细节，以便能够发现和识别数据集中的异常和模式 随着该领域的发展，学习新技术、工具和技术 收集、处理、保存、分析和呈现计算机相关证据，以支持网络漏洞缓解和/或犯罪、欺诈、反情报或执法调查	
合计		100

## 3.竞赛内容

### 3.1 考核内容

竞赛内容包括安全评估和操作技能两部分，竞赛成绩实行百分制，总成绩由两部分成绩加权合成。其中，操作技能成绩权重占 80%，安全评估成绩权重占 20%。

### 3.2 竞赛模块

模块 编号	模块名称	竞赛时间 min	分数		
			评价分	测量分	合计
A	网络安全事件响应	360	0	50	50
B1	漏洞评估与修复	150	10	10	20
B2	网络安全攻防	180	0	30	30

总计	690	10	90	100
----	-----	----	----	-----

### 3.3 模块简述

#### 3.3.1 模块 A：网络安全事件响应

选手需根据企业发现的安全事件，进行网络安全事件的调查、分析和取证，收集、保存、处理、分析和提取与计算机及网络相关的证据，并分析黑客的入侵行为。包括但不限于网络安全事件响应、数字取证调查、APK 分析、应用程序安全等。

#### 3.3.2 模块 B1：漏洞评估与修复

选手需进入预设的漏洞环境，识别系统、应用或配置中的安全问题，按照题目描述要求编写完整的漏洞报告。报告需包含漏洞描述、影响分析、风险评估及可行的修复方案，确保漏洞能被有效修补。考察选手对常见安全漏洞的理解、分析能力及修复建议的合理性。涉及领域包括但不限于 Web 安全、系统配置缺陷、应用安全缺陷、身份认证与访问控制问题、加密及数据保护漏洞等。

#### 3.3.3 模块 B2：网络安全攻防

选手需模拟攻击行为，运用所学的信息收集、漏洞发现和漏洞利用等技术，完成对目标网络的渗透测试。具体包括但不限于以下技术领域：数据库攻击、枚举攻击、权限提升攻击、基于应用系统的攻击、基于操作系统的攻击、逆向分析、密码分析、隐写分析等。

### 3.4 命题方式

本项目竞赛题的命题方式：

本项目为赛前需对试题保密的项目。赛前两周公布样题（包括赛题、素材、评分细则）。赛前，赛区组委会应商本赛区相关项目裁判长，参照本项目全国技能大赛试题命制、公布的方法和程序，结合国内保密工作管理要求，命制和公布试题，确保比赛公平、公正。

### 3.5 竞赛日程及地点安排

网络安全项目竞赛在南昌技师学院举行，竞赛时间暂定为 2025 年 4 月，具体时间以大赛正式通知为准。

网络安全项目竞赛正式时间为期 2 天，其中 C-1 为选手熟悉场地，C1 为 A 模块比赛，C2 为 B1、B2 模块。赛事日程安排如下所示：

#### 1.整体安排

时间	主要事项
C-2	裁判和选手报到
C-1	裁判赛前培训、裁判执裁分组、选手熟悉竞赛设备和竞赛环境、部署 A 模块环境
C1	A 模块比赛和评分，部署 B 模块环境
C2	B1 模块、B2 模块比赛和评分，得分汇总统计
C+1	公布得分及名次，技术点评会；返程

#### 2.具体安排

##### C-2 时间安排表

时间	事项	参与人员	负责人
9:00-18:00	裁判和选手报到	裁判员，选手	承办院校

##### C-1 时间安排表

时间	事项	参与人员	负责人
9:00-12:00	赛前准备会议，裁判培训和分工	裁判长 全体裁判员	裁判长

时间	事项	参与人员	负责人
15:00-16:00	选手熟悉场地、竞赛设备和竞赛环境	裁判长 全体裁判员 选手	裁判长
16:00-17:00	设备设施恢复、最终试题 A 模块环境部署	裁判长 全体裁判员 场地经理	场地经理
17:00-17:30	封场	裁判长 场地经理	裁判长

C1 时间安排表

时间	事项	参与人员	负责人
8:00	工作人员、裁判报道	工作人员 裁判长 全体裁判员	承办院校
8:00-8:20	赛前裁判会议	裁判长 全体裁判员	裁判长
8:20-9:00	选手检录、抽签、裁判长赛前介绍	裁判长 全体裁判员 选手	裁判长
9:00-15:00	A 模块比赛	裁判长 全体裁判员 选手	裁判长
15:00-15:30	A 模块收卷	裁判长 全体裁判员 选手	裁判长
15:30-16:00	A 模块评分	裁判长 全体裁判员	裁判长
16:00-16:30	A 模块成绩确认	裁判长 全体裁判员 录分员	裁判长
16:30-18:30	B 模块环境部署	裁判长 场地经理 全体裁判员	裁判长
18:30-19:00	封场	场地经理	场地经理

C2 时间安排表

时间	事项	参与人员	负责人
8:00	工作人员、裁判报道	工作人员 裁判长 全体裁判员	承办院校
8:00-8:20	赛前裁判会议	裁判长 全体裁判员	裁判长
8:20-9:00	选手检录、抽签、裁判长赛前介绍	裁判长 全体裁判员 选手	裁判长
9:00-11:30	B1 模块比赛	裁判长 全体裁判员 选手	裁判长
11:30-12:30	中场休息	裁判长 全体裁判员 选手	裁判长
12:30-15:30	B2 模块比赛	裁判长 全体裁判员	裁判长
15:30-16:30	B1、B2 模块评分	裁判长 全体裁判员	裁判长
16:30-18:00	B 模块成绩确认	裁判长 全体裁判员 录分员	裁判长
18:00-18:30	清除数据，恢复设备	裁判长 场地经理 全体裁判员	裁判长

C+1 时间安排表

时间	事项	参与人员	负责人
9:00-11:00	裁判长宣布成绩、项目技术点评	选手 裁判长	裁判长

## 4.评分标准

本项目采用测量评分为主、评价分辅助，各模块的评分标准不公开。本次竞赛评分表参考世界技能大赛网络安全赛项的评分标准制定。

### 4.1 评价分（主观）

评价分（Judgement）打分方式：3 名裁判为一组，各自单独评分，计算出平均权重分，除以 3 后再乘以该子项的分值计算出实际得分（四舍五入，保留小数点后两位）。裁判相互间分差必须小于等于 1 分，否则需要给出确切理由并在小组长或裁判长的监督下进行调分。

权重表如下：

权重分值	要求描述
0 分	各方面均低于行业标准，包括“未做尝试”
1 分	达到行业标准
2 分	达到行业标准，且某些方面超过标准
3 分	达到行业期待的优秀水平

### 4.2 测量分（客观）

测量分（Measurement）打分方式：按模块设置若干个评分组，每组由 3 名及以上裁判构成。每个组所有裁判一起商议，在对该选手在该项中的实际得分达成一致后最终只给出一个分值。

### 4.3 评分流程说明

本项目是事后结果评分、所有选手成绩不并列，各参赛队的最终总成绩为 A 和 B1、B2 两个模块成绩之和，若选手总成绩并列，本赛项按照 A 模块和 B2 模块、B1 模块的顺序进行得分排序。首先根据 A 模块得分进行排序，若 A 模块得分相同，则根据 B2 模块得分进行排序；若 B2 模块得分相同，则根据 B1 模块得分进行排序。

## 4.4 统分方法

裁判长组织裁判遵循“公平、公正、公开”原则执裁，采取分组评分的方式进行评分，评判过程依照评分标准进行。为确保评分过程的公平性和公正性，评分过程采取回避制度，裁判评分时遇到自己的选手要回避，由其他裁判替补评分。无相应模块任务（评分项）的裁判不得干扰和影响其他裁判的评分工作。

裁判员完成所有参赛选手评分后，对本人参与的评判结果进行核对确认。裁判长负责复核总成绩，并将各队参赛选手成绩交该参赛队裁判员确认，各裁判员最终签字确认本参赛队的选手成绩。

如在执裁和评分过程中出现争议的，由裁判长组织全体裁判讨论，以获得半数以上票数为裁定结果。

## 4.5 裁判构成和分组

### 4.5.1 裁判组

裁判长：裁判长由大赛组委会另行确定后公布；

裁判员：一般由参赛代表队派专业人员组成，各参赛代表队限派 1 人。

### 4.5.2 裁判任职条件

裁判员应具有团队合作、秉公执裁等基本素养，原则上须具备下列条件之一：

- 1.思想品德优秀，身体健康，年龄原则上不超过 60 岁；
- 2.具有本职业（赛项）高级工及以上职业资格或中级及以上专业技术职务；
- 3.有省级以上职业技能竞赛相关技术工作经历；
- 4.具备省级职业技能竞赛裁判员资格；
- 5.省级赛事技术专家。

裁判员需参加本项目赛前培训方可上岗。

### 4.5.3 裁判长职责

- 1.全面负责竞赛技术、裁判及争议处置等工作。



2.解读竞赛赛题及技术文件，牵头组织开展裁判员培训会议。

3.以分组形式安排裁判组任务分工，监督裁判员各项工作。

4.现场裁定有关裁判争议，协助仲裁组做出仲裁处理。

5.对扰乱赛场秩序，干扰裁判员工作，经裁判长讨论后酌情扣分，情况严重者取消竞赛资格。

6.裁判长在裁判员测评中，可进行抽查，若出现失职，第一次进行警告，同时对本代表队选手按规定给予扣分处罚，第二次取消执裁资格。

7.比赛过程中，A、B模块由裁判小组随机进行评测，小组签字后交给裁判长，再由裁判长审核后交由工作人员进行分数汇总，最终成绩由裁判长公布。

#### 4.5.4 裁判员职责

1.按照裁判长分组分工，具体承担比赛现场赛务工作，公平公正开展具体裁判和测评工作，并对本小组承担执裁工作的评判结果签字确认。

2.查看选手身份证和随身佩戴的对应工位号。

3.组织选手在赛前检查环境、设备、工具等，选手签字确认，审核选手自带设备工具是否符合要求，保障选手人身安全和设备正常使用。

4.协助裁判长解答技术及考核工作问题。

5.详实记录选手考核过程，及时提出意见建议。

6.遵照执行考核回避、保密等规则及议定事项。

7.接受裁判长和监督仲裁组的抽查和监督。

#### 4.5.5 裁判评判工作及纪律要求

1.裁判员出入赛场要佩戴胸牌，衣着整齐，举止大方，不大声喧哗，听从指挥，按照裁判长统一安排分组开展工作。

2.裁判员要严格遵守保密规定，正式比赛期间，不允许携带通信设备、智能设备、存储设备，比赛期间，不允许泄

露任何比赛信息，不允许单独离开赛场或单独与场外人员交流沟通。

3.裁判过程中实行回避政策，各代表队推荐的裁判员不参与本代表队选手和本地区代表队选手的执裁、测量、评分等工作，不得与本代表队选手和本地区代表队选手现场交流、指导。

4.各项目裁判组在选手报到、检录阶段，要按照本项目比赛细则要求，对选手携带的工具等进行严格检查，避免选手违规携带物品进入赛场对比赛成绩造成影响。

5.每一阶段（模块）比赛结束，需参赛选手离场的，各项目裁判组要在裁判长带领下，会同技术保障组，对每个工位的设备、设施、比赛工件（成果）、工具、材料等进行全面检查，确认无误后统一安排选手退场。

6.执裁过程中，出现技术争议、测评争议等问题由裁判长负责解释并裁定。

**5.竞赛相关设施设备**

对选拔赛设备、仪器、工具和原材料的数量、技术参数、品牌要求等进行说明；对配套设施要求进行说明；若允许自带工具，则应对允许范围进行说明。

**5.1 场地设备**

序号	名称	数量	技术规格
1	虚拟化平台服务器	1 台	处 理 器 :CPU:2 X Intel Xeon Gold 5220 Processor/2.20 GHz/25MB/18C/36T/125 W/2UPI/2667 MHz/ 内存: Samsung M393A8G40MB2-CVF 16 X 2666MT/s DRx4 64GB1.2V ECC RDIMM 硬盘: SATA0: HGST HUS726T4T 3 X 4000.7 GB S.M.A.R.T Supported.
2	竞赛服务器	1 台	1、外形 2U2 路机架式，标配原厂导轨； 2、配置 2 颗英特尔至强金牌 6530 (2.1GHz/32-Core) 处理器 3、配置 16*32GBDDR5 内存； 4、配置独立硬件 Raid 阵列卡，缓存 4GB，支

序号	名称	数量	技术规格
			持 RAID0/1/10/5/6/50/60（超级电容）； 5、配置 4 块 1.92T SATA SSD 硬盘； 6、配置 2 个千兆网口，2 个万兆网口（满配光模块）； 7、配置 1+1 热插拔高效冗余电源模块，单电源功率 1500W；满配热插拔冗余风扇，支持 N+1 冗余； 8、管理：配置独立运维管理控制接口，具备远程监控图形界面，可实现与操作系统无关地对服务器的完全远程控制，包括远程的开机、关机、重启、虚拟拨号、虚拟光驱等操作。
3	测评服务器	1 台	处理器: CPU: Intel(R) Xeon(R) Silver 4116 CPU @ 2.10GHz 内存: Samsung 2X DDR4 32 GB 2400 MHz 硬盘: INTEL SSDSC2KB480G8 512G /HGST HUS722T2TALA604 2000G
4	选手机	1 台/选手	启天 M540-A013(C)（Windows 11 Home 64bit 简体中文版，SFF 7.4L 180W 85%，cpu5800H 3.2G 8C 16T，8GB DDR4 3200 SoDIMM，512GB SSD M.2 2280 G4v TLC OPA，智能云教室，USB 前 4 后 2，USB Calliope 黑色鼠标，USB 键盘，启天主机，21.5 寸 LED 液晶显示器）
5	千兆交换机	4 台	小组组网用
6	移动硬盘	1 个/组	1TB-SSD

## 5.2 材料（软件）

序号	软件名称	版本
1	Windows 10 x64	Enterprise LTSC
2	Linux(Ubuntu)	20.04.x LTS
3	splunk	9.x
4	Apache	2.4.x
5	ModSecurity	2.9.3
6	vsftpd	3.x
7	Wireshark	3.4.9
8	openssl	1.x

9	Kali	Version2021.3
10	IDA free	7.x
11	MariaDB	10.x
12	OllyDbg	Version1.10
13	Volatility	Version2.x
14	Autopsy	Version4.x
15	x64dbg	snapshot_2023-03-04_02-26
16	Jadx-gui	1.4.x
17	HxD Hex Editor	Version 2.x
18	StegSolve	1.4
19	audacity	3.1.0
20	pwndbg(GDB 插件)	2021.06.22
21	sagemath	9.1
22	Pwntools(python)	4.6.x
23	pyCryptodome(python)	3.14.x
24	Pillow (python)	8.1.2
25	vscode	X64
26	Word	Office 2019
27	Frp	0.38.0
28	Neo-reGeorg	v3.7.0
29	Putty	0.68
30	ultraVNC	1.4.x
31	CaptfEncoder	2.1.0
32	Cutter	2.x
33	CyberChef	v9.55.0

### 5.3 竞赛选手自备的设备和工具

选手不得携带任何资料进入竞赛区。

### 5.4 竞赛场地禁止自带使用的设备和材料

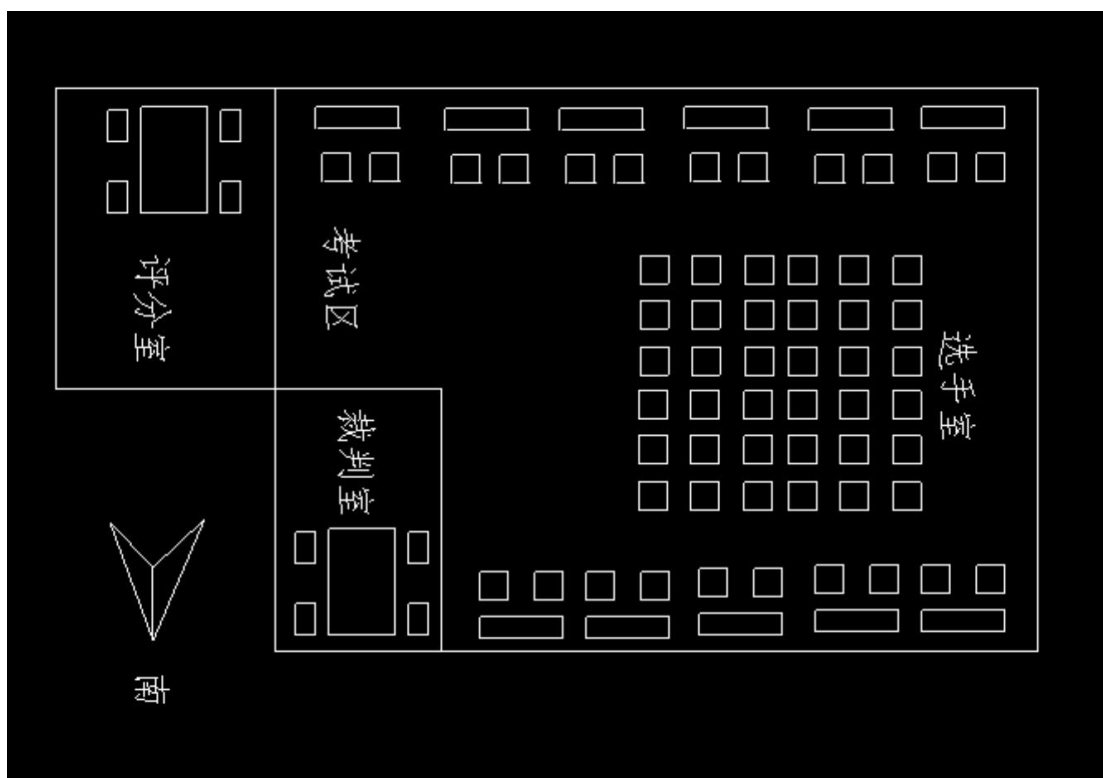
选手不得携带任何资料进入竞赛区。

## 6.项目特别规定

项目特别规定用于提供该赛项所特定的一些细则。项目特别规定包括但不限于：个人 IT 设备、数据存储设备、因特网接入、程序和 workflows、文档管理和发放，项目特别规定列表如下：

项目/任务	项目特别规定
使用技术/个人照相机	裁判任何情况下,不得携带个人照相机进入竞赛场地中的选手工位,除非由裁判长或裁判长助理批准 选手不得将照相机带入场地
使用技术/移动设备	裁判任何情况下,不得携带任何电子设备进入竞赛场地中的选手工位,除非由裁判长批准 选手电子设备(包括移动电话)必须存放在选手背包(关机或静音)并放于储物柜中。任何情况下,不得携带任何电子设备进入竞赛场地中的选手工位,除非由裁判长或裁判长助理批准
资源文件/笔记	选手任何情况下,不得携带笔记进入竞赛场地,竞赛期间在选手竞赛场地工位中记录的必须全程都留在选手桌上,不得将任何笔记带出竞赛场地
设备故障	选手如果出现设备故障,选手必须立即举手通知裁判,裁判应将选手因故障不能操作的时间记录在案;因设备故障导致的时间损失,将在模块的规定时间之外给予补时;因设备故障前未能存盘导致的时间损失将不予补时

## 7.赛场布局要求



具体赛场布局图以实际为准

## 8.健康安全和绿色环保

### (一) 选手安全防护要求

- 1.参赛选手应严格遵守设备安全操作规程。
- 2.参赛选手停止操作时，应保证设备的正常运行，比赛结束后，所有设备保持运行状态，不要拆、动硬件连接，确保设备正常运行和正常评分。

3.参赛选手应遵从安全规范操作。

4.参赛选手应保证设备和信息完整及安全。

### (二) 选手禁止携带物品

本次比赛赛场提供选手比赛所需的设备，选手除禁止携带任何带有存储功能的电子产品进入赛场外，还需禁止携带如下物品：

- 1.任何储存液体、气体的压力容器。
- 2.任何有腐蚀性、放射性的化学物品。
- 3.任何易燃、易爆物品。
- 4.任何有毒、有害物品。
- 5.任何没有生产厂商或达不到国家安全标准的工具及设备。
- 6.任何可能危及安全问题的物品。
- 7.任何影响竞赛公平性的物品。

### (三) 循环利用

耗材回收有序，设备循环使用，某些赛后产品留用给当地学校，作为技能培训使用。

## 9.开放赛场

### (一) 对于公众开放的要求

场馆开放，广泛宣传，要求注意各项安全。

比赛现场对社会开放，观众按照一定的安全要求，可以在赛场周围观看比赛。广泛向社会宣传技能人才培养和职业技能要求。

### (二) 工作人员守则

1.工作人员必须服从赛项组委会统一指挥，佩戴工作人员标识，认真履行职责，做好竞赛服务工作。

2.工作人员按照分工准时上岗，不得擅自离岗，应认真履行各自的工作职责，保证竞赛工作的顺利进行。

3.工作人员应在规定的区域内工作，未经许可，不得擅自进入竞赛场地。如需进场，需经过裁判长同意，核准证件，有裁判跟随入场。

4.如遇突发事件，须及时向裁判员报告，同时做好疏导工作，避免重大事故发生，确保竞赛圆满成功。

5.竞赛期间，工作人员不得干涉个人工作职责之外的事宜，不得利用工作之便，弄虚作假、徇私舞弊。如有上述现

象或因工作不负责任的情况，造成竞赛程序无法继续进行，由赛项组委会视情节轻重，给予通报批评或停止工作，并通知其所在单位做出相应处理。

### （三）安保须知

1.全体参赛人员要严格服从竞赛突发安全事故应急领导小组的指挥，比赛期间所有车辆、人员需凭证进入赛区，遵守赛场秩序，在规定区域内活动。

2.在竞赛开始前，选手要认真阅读《安保须知》和场地应急疏散图。

3.全体参赛人员一律不准在竞赛场所和禁烟区域吸烟。

4.严禁携带易燃易爆等危险品进入竞赛区域。

5.比赛期间如发生特殊情况，要保持镇静，服从现场工作人员指挥，按疏散通道有序撤离，保证参赛人员的安全。

6.安保人员发现安全隐患及时向赛项组委会报告。

### （四）对于赞助商和宣传的要求

经组委会允许的赞助商和负责宣传的媒体记者，按竞赛规则的要求进入赛场相关区域。上述相关人员不得妨碍、干扰选手竞赛，不得有任何影响竞赛公平、公正的行为。