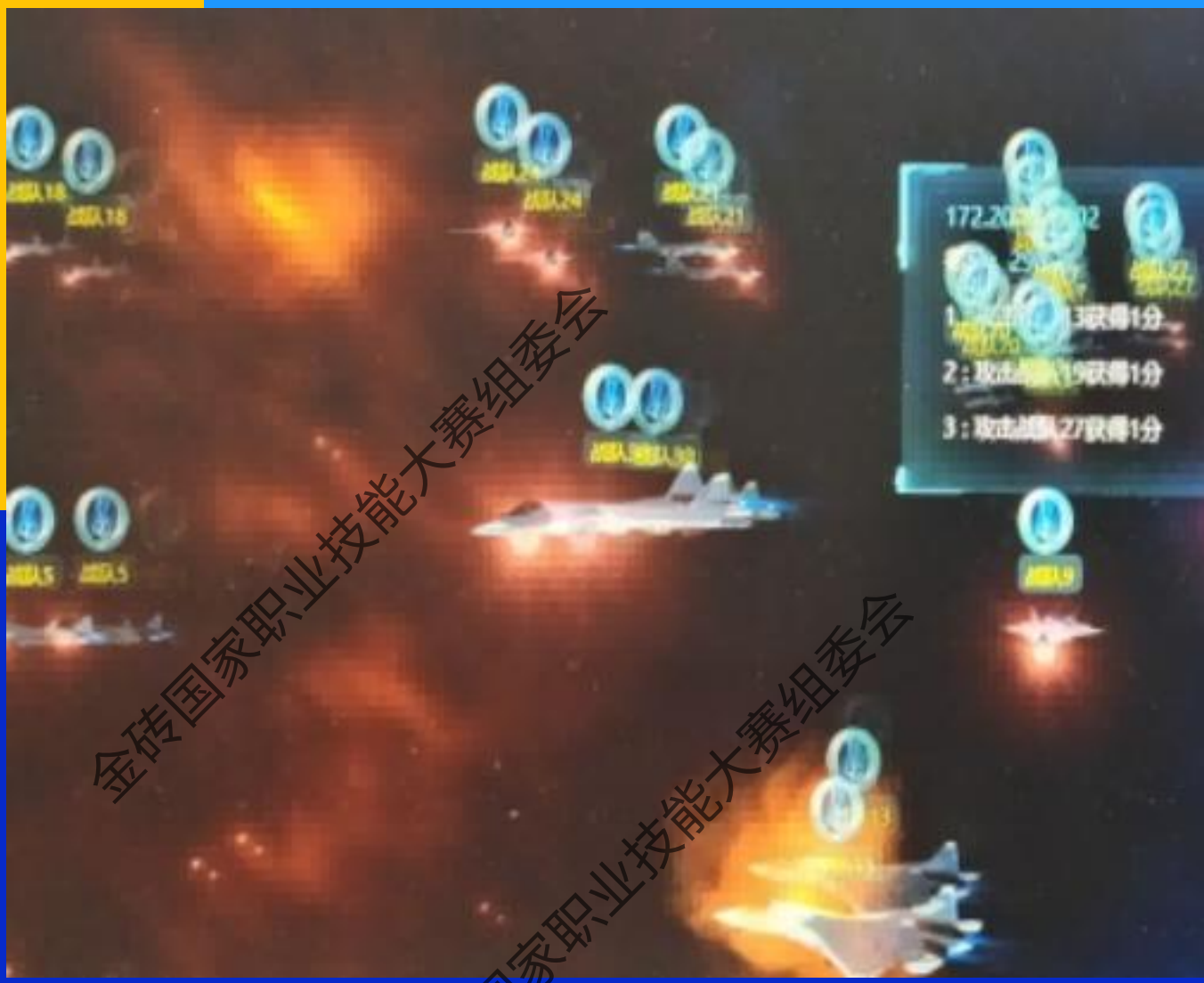
2022 年金砖国家职业技能大赛



技术说明（仅供选拔赛参考）

BRICS-FS-28_网络安全

目　录

1 简介

1.1 技能竞赛名称及说明

1.1.1 技能竞赛的名称

网络安全

1.1.2 技能竞赛描述

金砖国家职业技能网络安全竞赛项目旨在检验参赛选手安全运维、安全审计、网络安全应急响应、数字取证调查、应用程序安全和网络攻防渗透能力，检验参赛队计划组织和团队协作等综合职业素养，强调学生创新能力和实践能力培养，提升学生职业能力和就业质量。

本赛项以团队赛的方式进行，每队 3 名选手（设队长 1 名）。

通过团队合作，打通技术壁垒，实现相互赋能，促进网络安全产业国际化人才生态布局，加速网络安全与相关技术标准建设。秉承国际性顶级赛事“开放合作”的职业竞技精神，服务国家战略，深化产教融合，提升“国际化”建设水平，加速推进“岗课赛证”融合育人改革，以赛促建、以赛促改，切实增强职业教育适应性，培养具有国际视野、通晓国际规则的“国际化”技术技能人才，提高金砖五国职业技能竞赛工作水平和国际影响力。

1.1.3 竞赛系统

网络安全线下竞赛的开展将以网络安全技术线下培训与比赛系统为载体实现。

1.2 本文件的相关性和重要性

本文件包含本次技能竞赛所需的标准，以及管理竞赛的评测原则、方法和程序的信息。

每位专家和选手都必须了解和理解本技术说明。

如果不同语言的技术说明之间有任何冲突，以英文版本为准。

2 技能标准

2.1 技能标准的一般说明

技能标准规定了知识、理解和特定技能，这些技能是国际上在技术和职业表现方面

的最佳实践。它将反映全球对相关工作角色或职业在工业和企业中代表什么的全球共识。

技能竞赛旨在反映该技能标准所描述的国际最佳实践，以及它所能达到的程度。因此，该标准是技能竞赛所需培训和准备的指南。

该标准分为不同的带有标题和参考编号的部分。

每个部分被分配总分的百分比，以表明其在标准中的相对重要性。这通常被称为“权重”。所有百分比的总和分值为 100。权重决定在评分标准中分值的分配。

通过测试项目，评分方案只对标准中列举的技能进行评测。他们将在技能竞赛的约束下尽可能全面地反映标准。

评分方案将在实际可能的范围内按照标准中分配的分值进行。允许有 5%的变动，但不得改变标准规范分配的权重。

2.2 技能标准

2.2.1 技能标准的一般规范

标准规范	
1	**工作组织和管理**
	应知道并理解：
	健康与安全相关法规、义务、规定
	必须使用个人防护用品的场合，如：静电防护、静电放电
	在处理用户设备和信息时的诚信和安全的重要性
	废物回收、安全处置的重要性
	计划、调度和优先处置的方法
	在所有的工作实践过程中，注重准确、检验和细节的重要性
	系统性开展工作的重要性
	工作环境的 6S 管理
	应能够：
	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
	遵守相关规定，规划工作区域，维持日常整洁，实现最大化工作效率
	有效地工作，并定期检查进度和结果
	采取全面有效的研究方法，确保知识不断更新
	主动尝试新方法、新系统和愿意接受变革

2	**安全规定条款**
	应知道并理解：
	信息技术风险管理标准、政策、要求和过程
	网络防御和漏洞评估工具的功能和使用方法
	操作系统的具体功能
	计算机编程相关概念，包括计算机语言、编程、测试、调试、删除和文件类型
	应用于软件开发的网络安全和隐私原则和方法
	应能够：
	在设计总体程序测试和记录评估过程时，应将网络安全和隐私原则应用于管理要求(与保密性、完整性、可用性、身份验证、数字签名不可 抵赖性相关)
	对管理、操作和技术安全控制进行独立全面的评估，并对信息技术系统内部或继承的控制改进进行评估，以确定控制的整体有效性
	开发、创建和维护新的计算机应用程序、软件或专门应用程序
	修改现有的计算机应用程序、软件或专门应用程序
	分析新的或者现有计算机应用程序、软件或专业的应用程序的安全状况，提供可用的分析结果
	进行软件系统研究并开发新功能，确保有网络安全防护功能
	进行综合技术研究，对网络安全系统中可能存在的薄弱环节进行评估
	计划、准备和实施系统测试
	根据技术规范和要求，进行分析、评估并形成报告结果
	测试和评估信息系统的安全情况，涵盖系统开发生命周期
3	**操作、维护、监督和管理**
	应知道并理解：
	查询语言，如 SQL（结构化查询语言）
	数据备份和恢复，数据标准化策略
	网络协议，如 TCP/IP、动态主机配置(DHCP)、域名系统(DNS)和目录服务
	防火墙概念和功能
	网络安全体系结构的概念，包括拓扑、协议、组件和原则
	系统、网络和操作系统加固技术
	管理信息技术、用户安全策略（例如：帐户创建、密码规则、访问控制）
	信息技术安全原则和方法
	身份验证、授权和访问控制方法

	网络安全、漏洞和隐私原则
	学习管理系统及其在管理学习中的应用
	网络安全法与其他相关法规对其网络规划的影响
	应能够：
	管理数据库或数据库管理系统
	管理并实施流程和工具，确保机构可以识别、存档、获取知识资产和信息内容
	处理问题，安装、配置、排除故障，并按照客户需求或咨询提供维护和培训
	完成采集数据的准确性验证
	安装、配置、测试、运行、维护和管理网络和防火墙，包括硬件和软件，确保所有信息的共享、传输，对信息安全和信息系统提供支持
	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
	管理账户、设置防火墙和安装操作系统补丁程序
	访问控制、账户和密码的创建和管理
	检查机构的现有计算机系统和流程，帮助该机构更安全、更快捷和更高效的运营
	协助监督信息系统或网络，管理机构内部的信息安全可能存在的问题或其他需要负责的各方面，包括策略、人员、基础架构、需求、政策执行、应急计划、安全意识和其他资源。
4	**保护和防御**
	应知道并理解：
	文件系统实施(例如,新技术文件系统[NTFS]、文件分配表[FAT]、文件扩展名[EXT])
	系统文件(例如：日志文件、注册表文件、配置文件)包含相关信息以及这些系统文件存储位置
	网络安全体系结构的概念，包括拓扑、协议、分层和原理
	行业技术标准和分析原则、方法和工具
	威胁调查、报告、调查工具和法律、法规
	网络安全事件类别、响应和处理方法
	网络防御和漏洞评估工具及其功能
	对于已知安全风险的应对措施
	身份验证、授权和访问方法
	应能够：
	使用防护措施和利用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

	测试、实施、部署、维护、检查、管理硬件基础架构和软件，按要求有效管理计算机网络防护服务提供商的网络和资源
	监控网络，及时记录未授权的活动
	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和潜在的威胁
	使用缓解措施、准备措施，按照要求做出响应和实施恢复，以最大化存活率保障财产和信息的安全
	调查和分析相关网络安全应急响应活动
	对威胁和漏洞进行评估
	评估风险水平，制定在业务和非运营情况下采取适当的缓解措施
5	**分析**
	应知道并理解：
	网络威胁行为者的背景和使用的方法
	用于检测各种可利用的活动的方法和技术
	网络情报信息收集能力和资源库
	网络威胁和漏洞
	网络安全基础知识(例如，加密、防火墙、认证、诱捕系统、外围保护)
	漏洞信息传播源(例如，警报、通知、勘误表和公告)
	开发工具的结构、方法和策略(例如，嗅探、记录键盘)和技术(例如，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)
	预测、模拟威胁和应对的内部策略
	内部和外部协同的网络操作和工具
	系统伪造和司法用例
	应能够：
	识别和评估网络安全罪犯活动
	出具调查结果，以帮助初始化或支持执法和反情报调查或活动
	分析搜集到的信息，找到系统弱点和潜在可被利用的环节
	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。
	根据背景情况，同步和放置情报信息，找出可能的含义
	应用来自一个或多个不同国家、地区、组织和技术领域的最新知识
	应用语言、文化和技术专业知识进行信息收集、分析和其他网络安全活动
	识别、保存和使用系统开发过程遗留物并用于分析

6	**收集与操作**
	应知道并理解：
	收集策略、技术及工具应用
	网络信息情报收集能力和资源库的利用
	信息需求和收集需求的转换、跟踪、优先排序
	网络运营计划方案、策略和有关资源
	网络运营策略、资源和工具
	网络运营的概念、网络运营术语、网络运营的原则、功能、边界和效果
	应能够：
	运用适当的策略，通过收集管理的流程建立优先级，从而执行信息收集
	执行深入的联合目标定位，执行网络安全流程
	依照需求收集信息，执行详细计划及订单
	支持收集关于网络威胁的证据，减轻或免受可能的或实时的网络威胁
7	**调查**
	应知道并理解：
	威胁调查、报告、调查工具和法律、法规
	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，同时并维持监管链
	司法流程，包括事实陈述和证据
	持久性数据的类型和集合
	数字取证数据的类型和识别方法
	网络安全漏洞的具体操作性影响
	应能够：
	收集、处理、保存、分析和提供计算机相关的证据，以减轻网络脆弱性，支持犯罪、欺诈、反间谍或执法的调查

2.2.2 技能标准的详细文件

该赛项涉及的网络安全工程在设计、组建过程中，主要有以下 18 项标准，参赛队在实施竞赛项目中要求遵循如下规范：

序号	标准号	中文标准名称

1	WSC2022_WS0554_Cyber_Security	《世界技能大赛网络安全项目职业标准》
2	GB / T 22239-2019	《信息安全技术网络安全等级保护基本要求》
3	GB / T 28448-2019	《信息安全技术网络安全等级保护测评要求》
4	GB 17859-1999	《计算机信息系统安全保护等级划分准则》
5	GB/T 20271-2006	《信息安全技术信息系统通用安全技术求》
6	GB/T 20270-2006	《信息安全技术网络基础安全技术要求》
7	GB/T 20272-2006	《信息安全技术操作系统安全技术要求》
8	GB/T 20273-2006	《信息安全技术数据库管理系统安全技术要求》
9	GA/T 671-2006	《信息安全技术终端计算机系统安全等级技术要求》
10	GB/T 20269-2006	《信息安全技术信息系统安全管理要求》
11	ISO OSI	OSI 开放系统互连参考模型
12	IEEE 802.1	局域网概述，体系结构，网络管理和性能测量
13	IEEE 802.2	逻辑链路控制 LLC
14	IEEE 802.3	总线网介质访问控制协议 CSMA/CD 及物理层技术规范
15	IEEE 802.6	城域网（Metropolitan Area Networks)MAC 介质访问控制协议 DQDB 及其物理层技术规范
16	IEEE 802.10	局域网安全技术标准
17	IEEE 802.11	无线局域网的介质访问控制协议 CSMA/CA 及其物理层技术规范
18	ISO/IEC 27001	《信息安全管理体系》

2.2.3 赛项涉及知识点与技能点

序号	内容模块	说明
第一阶段（理论）	职业素养	网络安全规范意识、安全意识、纪律意识等
	网络安全	路由器、交换机、防火墙、日志审计、入侵检测等安全组网安全设备管理与安全配置等； 防火墙路由、安全策略、NAT、VPN 等配置和测试； 网络日志系统网络检测、统计、告警等配置； web 应用防火墙防护策略、过滤策略、告警等配置； 无线管理、无线 网络设置、安全策略等配置和测试； 三层交换机路由、 二层安全等配置和测试；
	安全运营	Windows Server 系统与 Linux 系统安全运营知识点考核；
	应急响应	操作系统和应用系统的日志分析，漏洞分析，系统进程分析，内存分析，系统安全加固，程序逆向分析，编码转换，加解密技术，数据隐写，文件分析取证，网络流量包分析，移动应用程序分析，代码审计等常用渗透与防护管理知识点考核；
第二阶段	安全运营	**Server 系统安全运营管理：** 系统安全运营、数据库安全运营、Web 安全运营、数据完整性保护、应用安全运营、防护墙安全管理、事件监控
		Linux 系统安全运营管理： 系统安全运营、数据库安全运营、Web 安全运营、数据完整性保护、应用安全运营、防护墙安全管理、事件监控
第三阶段	应急响应	**安全事件应急响应：** 系统日志分析、进程分析、内存文件分析、木马病毒分析 程序逆向分析、移动应用程序代码分析、恶意脚本分析
		数字取证与调查： 网络流量分析、协议流量分析、文件分析取证 编码转换、加解密、数据隐写
第四阶段	CTF 夺旗	**CTF 夺旗：** 漏洞渗透测试及其安全编程 SQL Injection（SQL 注入） 漏洞渗透测试及其安全编程 Command Injection（命令注入） 漏洞渗透测试及其安全编程 File Upload（文件上传） 漏洞渗透测试及其安全编程 Directory Traversing（目录穿越） 漏洞渗透测试及其安全编程 XSS（Cross Site Script） CSRF（Cross Site Request Forgeries） Cookie Stole（Cookie 盗用） 人工智能在信息安全中的应用 日志和网络流量的分析及应用 应用服务漏洞利用 二进制漏洞利用 逆向文件分析 密码学分析

3 评分方案

3.1 评分方法

本赛项四个阶段均为计算机自动评分，赛场赛场内需进行两次加密，提交成绩需进行三次加密。加密裁判组织实施加密工作，管理加密结果。监督员全程监督加密过程。

第一组加密裁判：组织参赛选手进行第一次抽签，产生参赛编号，替换选手参赛证等个人身份信息，填写一次加密记录表连同选手参赛证等个人身份信息证件，装入一次加密结果密封袋中单独保管。

第二组加密裁判：组织参赛选手进行第二次抽签，确定赛位号，替换选手参赛编号，填写二次加密记录表连同选手参赛编号，装入二次加密结果密封袋中单独保管。

第三组加密裁判：对参赛选手提各阶段绩进行第三次加密，将加密后的结果，交由裁判长组织评分裁判进行评分汇总。第三次加密过程文件由加密裁判密封保存，单独保管。

所有加密结果均需由相应加密裁判和监督人员签字。

四个阶段成绩汇总解密后由裁判长进行复核签字后，由裁判长确认后交工作人员录入系统。

3.2 评分规则

3.2.1 裁判评分方式

现场裁判组监督现场机考评分，评分裁判负责参赛各阶段成绩加密，裁判长负责成绩解密汇总及竞赛全过程。

竞赛现场派驻监督员、裁判员、技术支持队伍等，分工明确。现场裁判员负责与参赛选手的交流沟通及试卷等材料的收发，负责设备问题确认和现场执裁；技术支持工程师负责所有工位设备应急，负责执行裁判确认后的设备应急处理。

3.2.2 成绩产生办法

赛按任务评分，满分为 1000 分，详细评分要求见下表。

竞赛阶段	阶段名称	任务阶段	评分方式
第一阶段 权重 10%	职业素养与理论技能	题 1…N	机考评分
第二阶段 权重 30%	安全运营	任务 1…N	机考评分

第三阶段 权重 30%	应急响应	任务 1…N	机考评分
第四阶段 权重 30%	CTF 夺旗	任务 1…N	机考评分

3.2.3 排名规则

第三组加密裁判：对参赛选手提各阶段绩进行第三次加密，将加密后的结果，交由裁判长组织评分裁判进行评分汇总。第三次加密过程文件由加密裁判密封保存，单独保管。按照四个阶段汇总成绩。按照成绩排名，如果分数相同，比对第四阶段成绩，成绩高者排名靠前。若总分相同、第四阶段成绩相同，比对第三阶段成绩，成绩高者排名靠前，依次类推。

4 竞赛项目要求

4.1 常见注意事项

（一）竞赛期间禁止携带使用移动存储设备、计算器、通信工具及参考资料。

（二）请根据大赛所提供的竞赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

（三）在进行任何操作之前，请阅读每个部分的所有任务。各任务之间可能存在一定关联。

（四）操作过程中需要及时按照答题要求保存相关结果。竞赛结束后，所有设备保持运行状态，评判以最后提交的成果为最终依据。

（五）竞赛完成后，竞赛设备、软件和赛题请保留在座位上，禁止将竞赛所用的所有物品（包括试卷等）带离赛场。

（六）禁止在提交资料上填写与竞赛无关的标记，如违反规定，可视为0分。

4.2 竞赛时间安排与分值权重

“网络安全”竞赛共分四个阶段：第一阶段：职业素养与理论技能；第二阶段：网络安全运营；第三阶段：网络安全事件应急响应；第四阶段：CTF 夺旗挑战。

竞赛时间安排和分值权重见下表：

竞赛阶段	阶段名称	竞赛时间（分钟）	权重	评分方式
第一阶段	职业素养与理论技能	第一天上午 90 分钟	10%	机考评分
第二阶段	安全运营	第一天下午 210 分钟	30%	机考评分

第三阶段	应急响应	第二天上午 210 分钟	30%	机考评分
第四阶段	CTF 夺旗	第二天下午 210 分钟	30%	机考评分
合计		720 分钟	100%	

4.3 各模块作业内容及要求

竞赛内容涵盖网络安全设备安全管理、岗位职业素养与技能、网络安全运营管理、系统安全运营管理、安全事件应急响应、CTF 夺旗攻防等内容，综合考查参赛选手网络安全项目综合能力。

第一阶段：职业素养与理论技能；

第二阶段：网络安全运营；

第三阶段：网络安全事件应急响应；

第四阶段：CTF 夺旗挑战。

序号	内容模块	考核内容说明	考核形式
第一阶段	职业素养	网络安全规范意识、安全意识、纪律意识等；	单选/多选/判断题
	网络安全	路由器、交换机、防火墙、日志审计、入侵检测等安全组网安全设备管理与安全配置等； 防火墙路由、安全策略、NAT、VPN 等配置和测试； 网络日志系统网络检测、统计、告警等配置； web 应用防火墙防护策略、过滤策略、告警等配置； 无线管理、无线 网络设置、安全策略等配置和测试； 三层交换机路由、 二层安全等配置和测试；	
	安全运营	Windows Server 系统与 Linux 系统安全运营知识考核；	
	应急响应	操作系统和应用系统的日志分析，漏洞分析，系统进程分析，内存分析，系统安全加固，程序逆向分析，编码转换，加解密技术，数据隐写，文件分析取证，网络流量包分析，移动应用程序分析，代码审计等常用渗透与防护管理知识点考核；	
第二阶段	安全运营	Windows Server 系统安全运营管理： 系统安全运营、数据库安全运营、Web 安全运营、数据完整性保护、应用安全运营、防护墙安全管理、事件监控	操作题

		Linux 系统安全运营管理： 系统安全运营、数据库安全运营、Web 安全运营、数据完整性保护、应用安全运营、防护墙安全管理、事件监控；	
第三阶段	应急响应	安全事件应急响应： 系统日志分析、进程分析、内存文件分析、 木马病毒分析； 程序逆向分析、移动应用程序代码分析、 恶意脚本分析；	
		数字取证与调查： 网络流量分析、协议流量分析、文件分析取证； 编码转换、加解密、数据隐写；	
第四阶段	CTF 夺旗	CTF 夺旗： SQL Injection（SQL 注入）； Command Injection（命令注入）； File Upload（文件上传）； Directory Traversing（目录穿越）； XSS（Cross Site Script）； CSRF（Cross Site Request Forgeries）； Cookie Stole（Cookie 盗用）； 人工智能在信息安全中的应用； 日志和网络流量的分析及应用； 应用服务漏洞利用； 二进制漏洞利用； 逆向文件分析； 密码学分析。	

5 技能管理与沟通

5.1 专家组

技能专家组由 1 位首席专家、副首席专家和各国选派的专家组成，共同负责共同进一步修订本赛项远程决赛技术文件以及日常技能管理。

5.2 讨论论坛

比赛前有关软硬件准备、考试环境部署等相关疑问，参赛方可进入网络安全竞赛平台中的交流群进行反馈。本赛项的训练交流，比赛前，比赛中以及比赛后交流等也将通过交流群开展。

6 安全要求

请参考金砖国家职业技能大赛组委会健康、安全及环境政策和规范。

7 材料与设备

7.1 基础设施清单

7.1.1 硬件及环境配备：

赛项执委会每组提供个人计算机 3 台（安装 Windows 操作系统），用以组建竞赛操作环境，为参赛选手提供解题过程中的工具软件，并安装 Office 等常用应用软件。

序号	软件	介绍
1	Windows 10	操作系统
2	Microsoft Office 2016/2019	文档编辑工具
3	VMware 15 或以上版本	虚拟机运行环境
4	超级终端 SecureCRT/putty	设备调试连接工具
5	谷歌 Chrome	浏览器

7.1.2 准备提供渗透测试机和靶机虚拟机环境：

序号	软件	介绍
1	Windows 7\Windows XP\Windows 10	Windows 客户机操作系统
2	Windows Server 2003\2008\2010\2012\2016\2018	Windows 服务器操作系统
3	Ubuntu\Debian\Kali	渗透测试机操作系统
4	Linux CentOS	Linux 服务器操作系统

7.1.3 场地硬件配置：

硬件	数量	具体配置	备注
网络安全竞赛平台	1	1、能完成基础理论答题、安全运营与加固、安全事件响应、网络安全数据取证、CTF 夺旗等知识、技能内容的竞赛环境实现，能有效支持 600 人规模，具备基于本规程竞赛内容同一场景集中答题环境。 2、2. 标配 2 个千兆以太口，Intel 处理器，大于等于 16G 内存，SSD 硬盘。可扩展多种虚拟化平台，支持集群管理，同步采用增量备份的方式，虚拟化管理采用标准 libvirt 接口；支持多用户并发在线竞赛， 根据不同的实战任务下发进行自动调度靶机虚拟化模板，全程无需手工配置地址，VLAN 与 IP 可根据竞赛要求自行设定； 3、提供理论答题、安全运营、应急响应、CTF 夺旗四个阶段的竞赛模式，系统提供 500+的理论题库、提供 50+的安全运营、应急响应、CTF 夺旗不同题型场景；二三四阶段支持态势展示；阶段能进行成绩详细数据导出，平均分、正确率、答题情况、各任务得分情况数据统计展示；错题分析：展示易错题 TOP5、任务易错率、任务正确率等信息。	
交换机	若干	为各参赛队 PC 提供网络管理。	依据队伍数量而定
横幅或者大屏	1	CCVR 2022*** 分赛场”（***为学校的全称）	
备用配件	若干	电脑、摄像头、U 盘等	场地内部工位硬件损坏可随时进行更换
监控	1	手机或者录像机	比赛全程录制
电脑或者手机	1	Zoom 会议	用于与主赛场联络

7.1.4 网络配置：

项目	具体配置
网络配置	（线上赛可以联网，线下赛不支持联网） 工位电脑均支持连接互联网 ，带宽大于4M

7.2 建议的场地和工位布局

7.2.1 考位布置要求

（1）竞赛场地光线充足，照明良好；供电供水设施正常且安全有保障；场地整洁。

（2）竞赛场地设置隔离带，非裁判员、参赛选手、工作人员不得进入比赛场地。

（3）赛场设有保安、消防、医疗、设备维修待命，以防突发事件。

（4）赛场设置安全通道和警戒线，确保进入赛场的大赛参观、采访、视察的人员限定在安全区域内活动，以保证大赛安全有序进行。

7.2.2 移动监控设备的布置要求

移动监控设备 1 的中心线要求与比赛操作显示器平面呈 45°角，能监控到比赛操作显示器及选手侧脸，监控距离保证能监控到考位周边 1 米范围，高度 1.5 米左右。

移动监控设备 2 放置于考位桌上，其中心线要求与比赛操作显示器平面呈 45°角左右，要求其能最大限度地呈现完整的显示器比赛画面（显示器比赛画面尽可能地填充移动监控设备）