2025

金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）

网络安全

BRICS-FS-28

技术规程(国际总决赛)

2025 年 11 月

目录

1. 大赛简介 3
1.1. 大赛名称 3
1.2. 大赛目的 3
1.3. 报名资格 3
1.4. 赛制模式 3
2. 选手能力要求 4
3. 技能标准 5
3.1. 技能标准的一般说明 5
3.2. 技能标准的详细要求 5
3.3. 相关知识点参考文件 8
4. 知识大纲 10
5. 技能管理与沟通 14
5.1. 专家和裁判 14
5.2. 竞赛交流 15
6. 评分方案 15
6.1. 评分流程及方法 15
6.2. 评分规则 16
6.3. 排名规则 17
7. 竞赛项目要求 17
7.1. 注意事项 17
7.2. 竞赛时间安排与分值权重 17
8. 命题原则与事项说明 18
8.1. 命题原则 18

8.2. 答题方式 19
8.3. 竞赛赛题公布 19
8.4. 竞赛赛题改动 19
9. 大赛基础设施 19
9.1. 网络配置 20
9.2. 竞赛操作机硬件配置 20
9.3. 竞赛操作机软件配置 20
9.4. 竞赛平台及其他设备 21
9.5. 竞赛场地布局 22
10. 大赛纪律 23
11. 竞赛须知 24
11.1. 安全操作规定 24
11.2. 参赛队须知 25
11.3. 领队须知 25
11.4. 参赛选手须知 26
11.5. 工作人员须知 27

1. 大赛简介

1.1. 大赛名称

2025 金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）网络安全(Cyber Security)。

赛项编号：BRICS-FS-28

1.2. 大赛目的

2025 金砖国家职业技能大赛（金砖国家未来技能和技术挑战赛）网络安全赛项作为培育与锻造网络空间安全技术人才的关键平台，赛项紧跟网络空间安全攻防实战需求，致力于精准选拔具备实战能力的网络空间安全人才，着重对数字化转型进程中新技术融合场景下的网络空间安全风险，全面考核选手在安全规划设计、漏洞管理、应急响应处置及前沿技术安全治理等领域的综合能力。

1.3. 报名资格

2025 金砖国家职业技能大赛不设参赛组别，年龄在 16 周岁（2009 年 1 月 1 日以前出生）-35 周岁（1990 年 1 月 1 日以后出生）的职业院校（含高职本科、技工院校）及本科院校在校师生、企事业单位职工等均可作为参赛选手的身份报名参赛。

1.4. 赛制模式

大赛赛制采用 2 人赛模式，每队由 2 名选手组成。

2. 选手能力要求

重点考核参赛选手网络安全实战能力，包括网络安全理论及职业能力考核、网络与数据安全基础技能应用、网络安全运营技能应用、新技术、新应用领域产生的网络安全挑战（如可信数据空间安全）安全技能应用，具体包括：

（1）参赛选手需要具备网络安全法规与标准理解能力

掌握核心法律法规及标准规范,包括但不限于《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》及《网络与信息安全管理员（数据安全管理员）国家职业标准》等。

（2）参赛选手需要具备扎实信息技术基础知识与安全竞赛基础能力

掌握计算机硬件、软件、操作系统、数据库、网络协议等基础知识；具备网络与信息安全管理的基础素养；熟悉解题夺旗赛（CTF）的形式及其技术要求。

（3）参赛选手需要具备网络安全事件响应与取证分析能力

能够针对企业发现的安全事件，开展调查、分析与取证工作，具体包括：电子证据的收集、保存、处理、分析与提供；入侵行为的审计追踪；以及被破坏文件或系统的恢复。

（4）参赛选手需要具备渗透测试与漏洞挖掘实战能力

能够熟练运用各类渗透测试工具，对预设的网络靶场环境进行安全分析、漏洞挖掘和综合渗透，以模拟攻击者视角发现和验证安全风险。

（5）参赛选手需要具备应对新兴技术安全威胁的检测与防护能力

针对可信数据空间安全为代表的新技术/新应用领域的安全挑战，具备专项的安全检测和安全防护能力。

3. 技能标准

3.1. 技能标准的一般说明

技能标准明确了知识、理解和特定技能的要求，这些技能代表了国际上在技术和职业表现方面的最佳实践，体现了全球对于相关工作角色或职业在工业和企业中的共识。

技能竞赛以该技能标准为导向，旨在展示参赛选手对国际最佳实践的掌握程度。竞赛的培训和准备均以此标准为依据，确保选手能够达到规定的技能水平。

该标准由多个部分组成，每部分都有明确的标题和参考编号。每部分在总分中占有一定的百分比，即权重，反映了其在标准中的重要性。所有部分的权重总和为 100%。权重的设定直接影响评分标准中分值的分配，从而确保竞赛评估的公平性和准确性。

竞赛题目和评分方案紧密围绕标准中列举的技能进行设计，力求在竞赛的条件下全面反映标准要求。评分时，将尽可能按照标准中规定的分值进行，允许存在 5%的误差范围，但必须保持标准规范分配的权重不变，以确保竞赛结果的可靠性和有效性。

3.2. 技能标准的详细要求

（1）网络安全法律法规

参赛选手应了解：《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》及《网络与信息安全管理员（数据安全管理员）国家职业标准》等。

参赛选手应掌握：具备将网络安全和隐私原则融入总体程序测试与评估过程的设计和记录的能力，涵盖保密性、完整性、可用性、身份验证及数字签名不可抵赖性等关键要素；能够独立全面地评估管理、操作和技术安全控制，精准判断信息技术系统内部及其集成控制的有效性；具备开发、维护计算机应用程序、软件的能力，包括新建与修改，同时能够分析其安全状况并提供可靠结果；具备开展软件系统研究的能力，能够开发具备网络安全防护功能的新功能，评估网络安全系统薄弱环节；依据技术规范和要求，具备计划、实施系统测试的能力，能够进行分析评估并形成报告，全面测试信息系统安全，覆盖系统开发生命周期。

（2）基础网络安全攻防实战

参赛选手应了解：操作系统基础（Linux 文件和目录结构、环境安装部署等）、基础命令、配置与管理，以及 Linux 文件系统、Shell 和文本操作；应用服务器原理、网页知识；网络各层协议及组网通信技术；脚本语言、PHP、Java、前端语言开发基础。

参赛选手应掌握：具备数据库及数据库管理系统管理的能力；能够实施流程和工具管理，保障机构知识资产和信息的有效性；具备问题处理能力，涵盖安装、配置、故障排除，依据需求提供维护培训；具备采集数据准确性验证的能力；具备网络和防火墙（软硬件）全生命周期管理的能力，保障信息共享传输安全；具备服务器（软硬件）管理的能力，确保信息三大属性；具备账户、防火墙、系统补丁管理的能力；具备访问控制及账户密码管理的能力；能够检查优化机构计算机系统和流程。

（3）安全事件应急响应

参赛选手应了解：行业技术标准、分析原则方法工具；威胁调查报告工具法规；网络安全事件分类处理方法；网络防御漏洞评估工具功能；已知安全风险应对；身份验证授权访问方法。

参赛选手应掌握：具备运用防护措施和多源信息识别分析报告网络事件的能力；具备管理硬件软件基础架构的能力，保障网络防护服务；具备监控网络记录未授权活动的能力；在专业领域具备有效响应危机降低威胁的能力；具备运用缓解准备措施响应恢复保障安全的能力；具备调查分析应急响应活动的能力；具备评估威胁漏洞的能力；能够依据风险水平制定业务非运营场景缓解措施。

（4）WEB 漏洞挖掘与防护

参赛选手应了解：网络威胁行为者背景方法；检测可利用活动技术；网络情报收集能力资源；网络威胁漏洞；Web、服务器漏洞及探测工具原理；各类漏洞利用方法及提权原理。

参赛选手应掌握：具备使用漏洞探测工具精准探测各类漏洞的能力；具备运用技术手段进行弱口令爆破、敏感文件获取、数据库信息提取、恶意代码注入执行等操作的能力；熟练掌握并运用常用渗透工具的能力。

（5）威胁分析与调查取证

参赛选手应了解：威胁调查报告工具法规；恶意软件分析；电子证据处理流程及监管链维持；司法流程及证据要求；数据类型及取证方法；漏洞具体影响。

参赛选手应掌握：具备规范进行计算机证据收集处理保存分析的能力，助力调查并减轻网络脆弱性。

（6）新技术、新应用领域网络安全挑战

参赛选手应了解：在新技术、新应用场景下数据安全面临的核心挑战，包括：复杂环境（如多源、跨系统/地域流动）中的数据面临的非授权访问、窃取、泄露风险；新架构（如云原生、边缘计算）带来的信任边界模糊化导致的权限控制、隔离与审计挑战；高级持续性威胁（APT）中的隐蔽数据窃取、滥用及精细的数据篡改与破坏风险；大规模数据聚合、关联分析导致的隐私侵犯与去匿名化风险；以及通过模型输出或系统特性可能引发的敏感原始数据泄露风险（如模型逆向、

成员推理攻击）。同时，需掌握关键合规要求，如重要数据识别与管理、数据分类分级标准（核心、重要、一般数据）以及《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等核心法规的基本原则（数据安全义务、个人信息处理规则、数据出境安全评估）和相关国家/行业标准在新场景下的适用性。

参赛选手应掌握：针对新技术、新应用场景，系统地开展数据安全风险评估，识别数据处理全生命周期（采集、传输、存储、处理、共享、发布、销毁）中的潜在风险点及关键数据资产威胁；基于风险评估和合规要求，设计并制定覆盖数据全生命周期的有效安全策略与措施（包括但不限于：数据最小化采集与脱敏/匿名化应用；设计细粒度、可审计的访问控制（如 RBAC/ABAC）与权限管理；规划并实施适用的数据传输（如 TLS）与静态存储加密；应用技术（如哈希、签名）保障数据完整性；设计安全的数据传输与共享机制；定义数据留存与安全销毁策略）；具备配置或集成主流数据安全技术（如 DLP、数据库审计、密钥管理、安全网关、日志审计分析等）来有效实施上述策略，保障数据的机密性、完整性和可用性；持续跟踪数据安全技术发展、新兴威胁态势及法规标准更新，主动学习以适应变化提升能力；快速识别、研判和响应数据泄露、非法访问、篡改、破坏等安全事件，有效执行应急响应流程进行处置、恢复。

3.3. 相关知识点参考文件

序号	知识点
1	习近平总书记关于网络强国的重要思想和关于网络安全工作的重要指示批示精神
2	《中华人民共和国网络安全法》
3	《中华人民共和国数据安全法》
4	《中华人民共和国密码法》

5	《中华人民共和国个人信息保护法》
6	《中华人民共和国刑法》《中华人民共和国治安管理处罚法》涉及网络安全违法犯罪相关条款
7	《数据出境安全评估办法》
8	《关键信息基础设施安全保护条例》
9	《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》
10	《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》
11	《GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南》
12	《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
13	《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》
14	《GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》
15	《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》
16	《GB/T 41391-2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》
17	《GB/T 41479-2022 信息安全技术 网络数据处理安全要求》
18	《GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南》
19	《GB/T 37094-2018 信息安全技术 办公信息系统安全管理要求》
20	《GB/T 40652-2021 信息安全技术 恶意软件事件预防和处理指南》
21	《GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南》
22	《GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南》
23	《GB/T 30276-2020 信息安全技术 网络安全漏洞管理规范》
24	《GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范》
25	《GB/T 37973-2019 信息安全技术 大数据安全管理指南》

26	《GB/T 37027-2018 信息安全技术 网络攻击定义及描述规范》
27	《GB/T 39204-2022 信息安全技术关键信息基础设施安全保护要求》
28	《网络与信息安全管理员（数据安全管理员）国家职业标准》
29	其他相关网络安全法律法规和标准规范

4. 知识大纲

“网络安全”竞赛共分四个阶段，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 30 分钟	25%	机考自动化评分
第二阶段	网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用	第一天上午 70 分钟	30%	机考自动化评分
第三阶段	网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析	第一天下午 90 分钟	35%	机考自动化评分
第四阶段	新技术、新应用领域产生的网络安全挑战（可信数据空间）	第一天下午 50 分钟	10%	机考自动化评分

	安全技能应用			
合计		240 分钟	100%	

（1）第一阶段：理论知识

知识点	说明
职业素养	涵盖网络安全规范意识、安全意识以及纪律意识等内容。要求参赛选手熟悉网络安全行业的准则与最佳实践，主动预防安全风险，严格遵守工作和竞赛纪律，按时完成各项任务。
法律法规	包含《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》等法律法规，以及其它与网络和数据安全相关的法律法规和标准规范。参赛选手需深入理解这些法律法规，确保在网络安全实践中的合法合规性。
漏洞挖掘知识点	包括 Web 漏洞原理知识，如 SQL 注入、跨站脚本（XSS）、跨站请求伪造（CSRF）等，以及服务器漏洞原理知识。同时，还需掌握各类漏洞的基本利用方法，例如利用弱口令进行爆破、利用文件类漏洞获取或上传敏感文件、利用命令执行漏洞运行恶意命令、利用 SQL 注入漏洞获取数据库信息等。
数据安全知识点	涉及数据安全法规政策、基础理论、技术理论、管理流程、安全评估以及个人数据安全意识等方面。参赛选手需了解数据安全相关的法规政策，掌握数据的完整性、保密性、可用性等基础理论，熟悉加密、访问控制、数据备份等技

	术理论，知晓数据生命周期管理、数据分类分级等管理流程，能够评估数据安全风险并制定防护措施，同时提高个人数据安全意识。
应急响应知识点	要求参赛选手掌握应急响应的原理流程与排查方法。在 LINUX 和 Windows 系统中，能够进行账户排查，包括特权账户和影子账户；网络通信与端口排查，使用相关工具查看网络连接；进程分析，通过命令分析系统进程；启动项分析，检查系统启动项；定时任务排查，查看 crontab 等定时任务；服务分析，分析系统服务；Webshell 排查，检测 Webshell 文件；系统后门排查，查找系统后门；还能识别常见 web 漏洞攻击特征、敏感信息漏洞利用特征以及 sql 注入漏洞利用特征等。
安全加固知识点	在 Windows 系统中，涉及账户与密码的安全策略设置，如设置强密码策略；用户和用户组的权限管理，合理分配用户权限；审核功能的启用，记录系统活动；以及利用日志和安全模板分析配置计算机。在 Linux 系统中，要求掌握账号和组的管理，了解弱口令密码的风险及检查方法，知晓检查空口令和系统中其它 id 为 0 用户的方法，熟悉 Linux 文件系统的文件格式分类。

（2）第二阶段：网络与数据安全技能应用

知识点	说明
网络攻防渗透与漏洞挖掘	要求参赛选手能够使用漏洞探测工具，准确探测 Web 漏洞、网络服务脆弱性以及服务器漏洞。具备利用漏洞进行攻击的能力，包括利用弱口令爆破，利用文件类漏洞获取

	敏感文件或上传恶意代码，利用命令执行漏洞运行恶意命令，利用 SQL 注入漏洞获取数据库信息，利用 XSS 漏洞实现恶意代码注入和执行，利用目录遍历漏洞访问任意文件，利用 XXE 漏洞执行探测和攻击，利用 CSRF 漏洞伪造请求，利用 SSRF 漏洞伪造请求，以及通过信息泄露漏洞访问敏感信息等。
数据安全分析与应用	主要考察选手的数据包分析和数据取证能力，包括检测和防止敏感信息泄露、对数据进行分类管理、应用数字水印技术保护数字内容版权和完整性，以及掌握常见加解密算法如 AES、RSA 等。

（3）第三阶段：网络安全运营技能应用

知识点	说明
网络安全事件响应	要求参赛选手掌握入侵检测、抑制处置、系统恢复和证据收集等知识点，并能够将其运用到实际操作中。能够及时发现入侵行为，采取有效措施阻止攻击进一步发展，迅速恢复系统正常运行，同时妥善收集和保存证据，为后续分析提供支持。
安全加固与溯源分析	安全加固方面，要求参赛选手掌握如何增强系统防御能力的方法，如合理配置安全策略、更新系统补丁、强化访问控制等。溯源分析则要求选手具备追踪攻击来源、分析攻击路径的能力，能够通过分析系统日志、网络流量等信息，还原攻击过程，找出攻击源头，为防范类似攻击提供依据。

（4）第四阶段：新技术、新应用领域的网络安全挑战

知识点	说明

可信数据空间安全	针对新技术、新应用场景，系统地开展数据安全风险评估，识别数据处理全生命周期（采集、传输、存储、处理、共享、发布、销毁）中的潜在风险点及关键数据资产威胁；基于风险评估和合规要求，设计并制定覆盖数据全生命周期的有效安全策略与措施（包括但不限于：数据最小化采集与脱敏/匿名化应用；设计细粒度、可审计的访问控制（如 RBAC/ABAC）与权限管理；规划并实施适用的数据传输（如 TLS）与静态存储加密；应用技术（如哈希、签名）保障数据完整性；设计安全的数据传输与共享机制；定义数据留存与安全销毁策略）；具备配置或集成主流数据安全技术（如 DLP、数据库审计、密钥管理、安全网关、日志审计分析等）来有效实施上述策略，保障数据的机密性、完整性和可用性；持续跟踪数据安全技术发展、新兴威胁态势及法规标准更新，主动学习以适应变化提升能力；快速识别、研判和响应数据泄露、非法访问、篡改、破坏等安全事件，有效执行应急响应流程进行处置、恢复。

5. 技能管理与沟通

5.1. 专家和裁判

成立技术专家组，技术专家组由精通网络安全技术的知名专家组成，职责是设计网络安全大赛技术架构。提供技术支持和咨询，以确保大赛的公平性和公正性。

成立裁判委员会，设裁判长 1 名（任命技术专家组组长为裁判长），裁判员

2 名，负责大赛现场的执裁、判分、监控及成绩核验确认等工作，并及时向大赛组委会办公室、评委会报告竞赛结果，现场发布竞赛成绩。

裁判委员会成员应具有团队合作、秉公执裁等基本素养，具有网络安全相关领域工作经验；有省级以上网络安全和信息化领域技能竞赛技术工作经历且在省级选拔活动中担任技术专家或具备国家职业技能竞赛裁判员资格。

5.2. 竞赛交流

比赛前若有软硬件准备、考试环境部署等疑问，参赛方可通过网络安全竞赛公众号与大赛赛项 QQ 群进行反馈。本赛项的训练交流、赛前、赛中及赛后交流等也通过公众号与 QQ 群开展。

6. 评分方案

6.1. 评分流程及方法

- 本赛项四个阶段均实行计算机自动评分，确保评分客观公正。在评分过程中，为保障信息安全，赛场内需进行两次加密操作。加密工作由专门的加密裁判负责，确保加密过程规范、准确。
- 第一组加密裁判负责首次抽签，产生参赛编号，替换选手个人身份信息，并记录加密过程，将相关证件装入密封袋单独保管。
- 第二组加密裁判组织第二次抽签，确定赛位号，替换参赛编号，并记录加密过程，将相关编号装入另一密封袋单独保管。
- 所有加密结果均须经加密裁判和监督人员签字确认，确保加密过程的透明性和可追溯性。
- 四个阶段成绩汇总解密后，由裁判长进行复核并签字确认，确保成绩的准确

性和公正性。最后，成绩由工作人员录入系统，完成整个评分流程。

6.2. 评分规则

- **裁判评分方式**

现场裁判组严密监督机考评分过程，确保公正公平。评分裁判负责各阶段成绩的加密工作，确保信息安全。裁判长则负责成绩的解密汇总，并全程把控竞赛进展。

竞赛现场配备监督员、裁判员和技术支持队伍，各司其职。裁判员负责与选手沟通，收发试卷等材料，处理设备问题；技术支持工程师则负责工位设备的应急处理，确保比赛顺利进行。

整个竞赛流程分工明确，团队协作紧密，为选手提供了良好的竞赛环境。

- **成绩产生办法**

竞赛按任务评分，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 25%	职业素养与理论技能	题 1…N	机考自动化评分
第二阶段 权重 30%	网络与数据安全技能应用，包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用	任务 1…N	机考自动化评分
第三阶段 权重 35%	网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析	任务 1…N	机考自动化评分
第四阶段 权重 10%	新技术、新应用领域产生的网络安全挑战（可信数据空间）安全技能应用	任务 1…N	机考自动化评分

6.3. 排名规则

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。

7. 竞赛项目要求

7.1. 注意事项

- 竞赛期间严禁携带移动存储设备、计算器、通信工具和参考资料。
- 请根据大赛提供的竞赛环境，检查硬件设备、软件及材料清单是否完整，确保计算机正常运行。
- 在操作前，请详细阅读所有任务要求，注意任务间可能存在的关联。
- 操作时请按答题要求及时保存结果。竞赛结束后，设备保持运行，最终提交成果为评判依据。
- 竞赛完成后，请保留设备、软件和赛题在座位上，禁止携带任何物品离场。
- 禁止在提交资料上添加与竞赛无关的标记，违规者将视为零分。

7.2. 竞赛时间安排与分值权重

“网络安全”竞赛共分四个阶段，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 30 分钟	25%	机考自动化评分
第二阶段	网络与数据安全技能	第一天上午 70 分钟	30%	机考自动化

	应用,包括基础网络攻防渗透与漏洞挖掘、数据安全分析与应用			评分
第三阶段	网络安全运营技能应用，包括安全事件响应、安全加固与溯源分析	第一天下午 90 分钟	35%	机考自动化评分
第四阶段	新技术、新应用领域产生的网络安全挑战(可信数据空间)安全技能应用	第一天下午 50 分钟	10%	机考自动化评分
合计		240 分钟	100%	

8. 命题原则与事项说明

8.1. 命题原则

（1）赛题均为原创赛题，并充分结合实际环境的理论和技术要求。

（2）赛题支持随机附件、动态 FLAG、理论题目顺序及选项均为随机等防作弊机制。

（3）为保障赛事公正性、公平性以及安全性，命题工作须严格按照大赛组委会办公室相关要求，全程保密，严禁赛题泄露。

8.2. 答题方式

（1）平台登录

参赛选手需要使用分配的账号、密码完成竞赛平台登录，确认账号可以正常登录竞赛平台。进入平台后可点击竞赛须知查看竞赛规则。（建议使用 Chrome 浏览器）

（2）理论题答题

点击理论题竞赛入口即可进入答题环节，每道题提交答案后可点击下一题作答。同时支持参赛选手自主选择任意题号进行作答，在理论题竞赛规定的答题时间内可修改答案。全部作答完毕后点击交卷完成理论题竞赛答题。

（3）CTF 答题

点击 CTF 竞赛入口即可进入答题环节，每道 CTF 题目需要解出正确 flag 值并提交后才可获得对应分值。可点击下一道题目继续作答，系统自动累加已获得题目的分值。

8.3. 竞赛赛题公布

竞赛赛题将会通过大赛官方网站，于赛前 1 个月左右进行公布。

官网地址：（http://www.brskills.com/jzzy/index.html）

8.4. 竞赛赛题改动

正式比赛前，竞赛赛题会进行约 30%的改动。

9. 大赛基础设施

大赛组委会办公室在竞赛场地搭建竞赛基础设施环境，包括：竞赛平台服务

器、UPS 电源、核心交换机、接入交换机、参赛选手 HUB、电源接线板以及竞赛观摩展示 LED 屏等。

9.1. 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

9.2. 竞赛操作机硬件配置

参数选手不需要自带电脑，大赛组委会办公室提供竞赛操作机。

设备	设备名称	数量	备注
参赛选手客户机	PC 机	根据参赛队伍配置	通用台式机（最低配置） 处理器：i5/i7 内存：16G 固态硬盘：256G 显卡：RTX4060 USB 接口：3.0 网卡：千兆

9.3. 竞赛操作机软件配置

序号	软件	介绍
1	Windows10	操作系统
2	MicrosoftOffice2016/2019	文档编辑工具
3	VMware17 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

9.4. 竞赛平台及其他设备

硬件	数量	具体配置	备注
网络安全竞赛平台	2	（1）竞赛平台系统采用 B/S 架构，内置题目管理、赛事管理、队伍管理、数据统计、大屏展示、数据运维等模块； （2）平台评分机制支持 FLAG 提交与选手 CHECK 验证两种模式，全程自动化完成赛事评分； （3）平台支持中英文界面展示，操作界面与题目描述都可以中英文展示，可支撑国际赛，也可以通过扩展支持第三种语言； （4）平台支持多种大赛类型，包括理论赛，CTF 夺旗赛，AWD/AWDP 攻防赛，安全运维赛等常见题型，可根据赛事要求灵活选择； （5）平台支持用户管理功能，提供账号管理、队伍管理、角色权限管理，管理员可对账户、队伍进行批量操作，包括导入、导出、新增、删除和禁用等操作； （6）平台支持多场竞赛同时管理，支持对竞赛新建、编辑、搜索、发布、环境部署、竞赛中管理、竞赛结果等流程进行操作；	主备配置，根据队伍数量可增加

		（7）平台支持个人及团体参赛方式的理论赛、解题赛、攻防赛竞赛模式，并可根据需求进行竞赛形式自由组合； （8）平台支持多场竞赛同时管理，支持对竞赛新建、编辑、搜索、发布、环境部署、竞赛中管理、竞赛结果等流程进行操作。	
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
横幅或大屏	1	金砖国家职业技能大赛 2025***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

9.5. 竞赛场地布局

竞赛场地光线明亮，照明设备完善；供电供水设施稳定可靠，场地保持整洁。

设置隔离带，限制非竞赛人员进入比赛场地，确保比赛区域的安全与秩序。赛场配备保安、消防、医疗及设备维修团队，随时待命，以应对突发状况。设立安全通道与警戒线，对进入赛场的参观、采访、视察人员进行区域限制，确保大赛安全有序进行。

10. 大赛纪律

参赛选手应严格遵守赛场纪律，服从指挥，统一佩戴参赛证，仪表端庄，讲文明礼貌。遵守赛场纪律，服从工作人员的指挥和安排，爱护比赛场地的设备和器材。

所有参赛选手须实名参赛，参赛时需携带身份证件。替考或虚报信息等行为一经查实，将被取消参赛资格并进行通报处理。

（1）参赛选手须在规定时间内入场，按照指定的机位号就座，入场后要服从竞赛组织者的统一安排，比赛开始后入场取消参赛资格。

（2）参赛选手必须在指定座位上完成比赛项目，未经裁判允许，不得擅自离开座位，如需去洗手间或有其他事项须举手示意，在工作人员确认及陪同下方可离席。

（3）竞赛过程中，参赛选手严禁向竞赛系统、其他参赛选手个人电脑等设备发起任何可能影响比赛的攻击行为。参赛选手须严格遵守操作规程，确保设备和人身安全，并接受裁判员的监督和警示。若因参赛选手因素造成设备故障或损坏，无法继续比赛，裁判长有权决定终止该参赛选手比赛；若因非参赛选手个人因素造成设备故障，由裁判长视具体情况做出裁决。

（4）参赛选手须严格遵守赛场规章制度，服从裁判，文明比赛，严禁各类串通作弊、与外界通信等严重违反竞赛纪律的行为。

（5）竞赛结束前，参赛选手不得提前退场；裁判宣布竞赛结束时，所有参赛选手应立即停止与答题相关的操作。

（6）竞赛采用系统自动评分，比赛过程中按照裁判要求操作，如有违规操作行为，按照作弊处理。

（7）为保证竞赛的公平、公正性，大赛组委会办公室专家组、裁判组将在比赛期间实时查看参赛选手的积分及排名变化，根据防作弊监测情况抽查参赛选手解题思路，各参赛选手解题时应将关键解题步骤（writeup）进行记录，并将全部题目的关键解题步骤（writeup）上传至竞赛系统。

（8）竞赛期间以裁判长的仲裁意见为最终裁决，如有不服从裁判、扰乱赛场秩序等不文明行为，将按照相关规定从严处理。

（9）违反上述规定者，现场裁判组将视情节进行处罚，处罚措施包括但不限于警告、扣分、取消比赛成绩、终止比赛资格并向所在单位通报等。对破坏竞赛基础环境，影响竞赛正常进行的，大赛组委会办公室将依法追究其责任。

（10）当听到大赛结束命令时，参赛选手应立即停止所有操作，不得以任何理由拖延比赛时间。离开比赛场地时，不得将比赛有关的物品带离现场。

11. 竞赛须知

11.1. 安全操作规定

（1）参赛选手须根据规定确认工位、设备、工具安全完好，严格遵守赛场 规章、操作规程，注意人身和设备安全，接受裁判员监督和警示，文明竞赛。

（2）参赛选手安装比赛设备时，应事先了解设备性能参数，确保正确使用 设备。

（3）参赛选手安装传感器等设备时，必须注意电源正负极短路，避免烧坏 设备，出现安全事故。

（4）参赛选手安装设备时，应保持工位电源关闭，不得带电连接设备。如 发现漏电等现象要及时报告裁判，联系技术人员查验设备。

（5）参赛选手在安装设备过程中要注意防静电安全，不得将电路板放在金 属表面及无防护堆叠。

（6）参赛选手请勿触碰和打开实训工位配电箱，注意工位后面 220V 强电使 用安全。

（7）参赛选手在比赛过程中不得进入其他参赛队工位，不得干扰其他参赛 队比赛。

11.2. 参赛队须知

（1）各参赛队须为参赛选手购买大赛期间的人身意外伤害保险。

（2）各参赛队须对参赛选手、领队进行安全管理和教育，领队在比赛期间 保持通信畅通。

（3）各参赛队应服从并执行仲裁结果。凡恶意申诉，一经查实，组委会将 追查相关人员责任。

（4）领队负责做好本参赛队比赛期间的管理与组织工作。

11.3. 领队须知

（1）领队要坚决执行竞赛和各项规则，服从赛项执委会的安排和管理，并 加强对参赛人员的管理，做好各项准备工作。

（2）领队负责抽取参赛队编号，比赛期间不得进入比赛现场。

（3）领队负责其参赛队赛事期间与大赛执委会的协调联络。

（4）参赛队如认为有不符合竞赛规定的事项发生时，由领队在比赛结束后 2 小时内向赛项仲裁组提交签字后的书面申诉材料。口头申诉无效，仲裁组不予受 理。

11.4. 参赛选手须知

（1）参赛选手应严格遵守赛场规章、操作规程，保证人身及设备安全，接 受裁判员的监督和警示，文明竞赛。

（2）参赛选手凭组委会颁发的参赛凭证和有效证件（身份证或护照）参赛。

（3）参赛选手按规定时间进入比赛场地，对现场条件进行确认并签字。按 统一指令进行操作。各参赛队自行决定选手分工、工作流程和时间安排，在规定时间内在指定工位上完成比赛。不得随意进入其他队的工位。

（4）参赛选手入场后根据规定确认竞赛设备、工具是否安全完好，严格遵 守赛场规章、操作规程，保证人身及设备安全。

（5）比赛过程中，若出现因非选手个人因素造成竞赛设备故障，请及时示 意现场裁判，由技术人员维修或更换竞赛设备。裁判组可视具体情况给予排除故 障所耗时间的补时。

（6）参赛选手安装部署竞赛设备时，请详细了解各设备性能参数，如供电 输入等，确保设备的正常使用。

（7）参赛选手连接传感器及其他设备时，注意防止正负极短路，避免烧坏 设备。请勿触碰和打开实训工位配电箱，注意工位后面 220V 强电使用安全。

（8）竞赛期间赛场统一提供食品、饮水。选手休息、饮食及如厕时间均计 算在比赛时间内。

（9）比赛结束后，参赛队需清理现场，将场地恢复到比赛前的状态。

（10）在比赛过程中，参赛选手如有不服从裁判指令，出现扰乱赛场秩序等 行为，由首席专家酌情扣减该参赛队成绩分数；情节严重的，取消比赛资格。有 作弊行为的，直接取消比赛资格。

11.5. 工作人员须知

（1）赛场工作人员由赛项执委会统一聘用并进行工作分工。

（2）服从赛项执委会的领导，遵守职业道德，坚持原则、按章办事。以高 度负责的精神、严肃认真的态度和严谨细致的作风做好工作。

（3）熟悉《赛项规程》，认真执行赛项规则。

（4）坚守岗位，不迟到、不早退、不擅离职守。

（5）赛场工作人员要积极维护好赛场秩序，以利于参赛选手正常发挥水平。

（6）工作人员在比赛中不回答选手提出的任何有关比赛的技术问题，如遇 争议问题，需上报执委会。

（7）因违反规定给比赛带来影响或造成损失的，将给予必要的处理。