第二届山东省职业技能大赛 网络安全项目技术工作文件

第二届山东省职业技能大赛

组委会办公室技术工作组

2025 年 05 月

目 录

一、技术描述	1
(一) 项目概要	1
(二) 基本知识与能力要求	1
二、试题与评判标准	6
(一) 试题 (样题)	6
(二) 比赛时间及试题具体内容	7
1. 比赛时间安排	7
2. 试题简述	7
(三) 评判标准	8
1. 竞赛试题配分	8
2. 成绩计算方式	9
3. 评判方法	9
三、竞赛细则	10
(一) 竞赛流程	10
(二) 裁判员须知	14
(三) 参赛选手须知	15
(四) 工作人员须知	17
(五) 成绩公布	18
(六) 技术违规处理	18
(七) 问题或争议处理	19
四、竞赛场地、设施设备等安排	19

(一) 赛场规格要求	19
(二) 场地布局图	20
(三) 基础设施清单	20
(四) 竞赛服务平台	22
1. 硬件环境	23
五、安全健康要求	24
(一) 选手安全防护要求	24
(二) 赛事安全要求	24
(三) 绿色环保要求	24
六、其他	25

一、技术描述

（一）项目概要

网络安全项目需要选手保护企业的信息系统，防止黑客访问和窃取企业的敏感数据。网络安全项目选手通常需要配置防火墙、入侵检测、服务器以及制定网站安全解决方案来保护企业的系统不被入侵。同时，他们还需要维护并实施企业的网络安全监控系统并调查发生在企业内部的网络安全事件。网络安全工程师需要对企业的信息系统进行安全渗透测试，提前发现可能被黑客利用的漏洞及时对漏洞进行修补和安全加固。

网络安全项目选手还需要能够保障虚拟基础设施的安全,开展相关信息安全活动，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的关键数据不被盗窃、修改和破坏。

选手需要进行数字调查取证，收集、保存、处理、分析和提供与计算机相关的证据，通过技术手段协助执法机构侦破网络犯罪和防止网络欺诈。

选手应同时具备表达、书写、沟通、协调等能力，具有较高综合素质。

（二）基本知识与能力要求

对选手理论知识、工作能力的要求以及各项要求的权重如下表：

相关要求		权重比例（%）
1	工作组织和管理	5
基本知识	个人（选手）需了解和理解： • 健康与安全相关法规、义务、规定。	

	<ul style="list-style-type: none"> • 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。 	
工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> • 遵守健康和标准、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	沟通 and 人际交往	
基本知识	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> • 倾听是有效沟通的重要手段。 • 团队成员的角色要求和最有效的沟通方式。 • 与团队成员和管理人员建立和保持创造性的工作关系的重要性。 • 有效的团队合作技巧。 • 消除误会和化解冲突的技巧。 • 管理紧张和愤怒情绪的能力。 • 团队合作的重要性。 	10
工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> • 运用认真倾听和提问的良好技巧，加深对复杂情境的理解。 • 与团队成员进行持续有效的口头和书面沟通。 • 认识到并适应团队成员不断变化的需求。 • 积极推动，建立强大而有效的团队。 • 与团队成员分享知识和专业知识，形成相互支持的学习文化。 • 有效管理不良情绪，传递给他人解决问题的信心。 • 与工作人员的沟通技巧。 	
3	安全规定条款	
基本知识	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> • 信息技术风险管理标准、政策、要求和过程。 	15

	<ul style="list-style-type: none"> • 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。 	
工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> • 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。 	
4	操作、维护、监督和管理	
基本知识	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> • 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。 	15

工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> • 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。 • 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。 	
5	保护和防御	
基本知识	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> • 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。 	15
工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> • 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 	

	<p>施恢复，以最大化存活率保障财产和信息的安全。</p> <ul style="list-style-type: none"> • 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。 	
6	分析	
基本知识	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> • 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。 	10
工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> • 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。 	
7	收集与操作	
基本知识	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> • 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。 	15

	<ul style="list-style-type: none"> 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。 	
工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> 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。 	
8	调查	
基本知识	<p>个人（选手）需了解和理解：</p> <ul style="list-style-type: none"> 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。 	15
工作能力	<p>个人（选手）应具备的能力：</p> <ul style="list-style-type: none"> 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。 	
合计		100

二、试题与评判标准

（一）试题（样题）

本次大赛以第 47 届世界技能大赛网络安全(Cyber Security)项目和中华人民共和国第二届职业技能大赛网络安全项目技术文件为指导，并参考世赛标准和国内行业实际来编制命题。本次比赛根据第 47 届世赛的比赛规则，公布技术路线，赛题、环境和素材均不公开，且不提供样题。赛前一天不对竞赛的赛题、环境和素材进行任何修改。具体比赛形式和样题可参考中华人民共和国第

二届职业技能竞赛样题。

本项目设置三个考核模块：

模块 A 企业基础设施安全；

模块 B 网络安全事件响应、数字取证调查和应用安全；

模块 C CTF 夺旗。

(二) 比赛时间及试题具体内容

1. 比赛时间安排

本项目比赛总时间为 9 个小时，分为 3 个模块 2 天完成，时间分配如下表：

模块编号	模块名称	竞赛时间 (小时)
A	企业基础设施安全	3
B	网络安全事件响应、数字取证调查和应用安全	3
C	CTF 夺旗	3
总计		9

2. 试题简述

模块A：任务根据实际信息安全服务的工作内容进行设计，以典型的组织机构信息系统网络架构为基础，相关的服务均可以正常运行，但不满足网络安全行业最佳实践。选手需要使用各种网络安全技术对已有的网络和服务进行配置和加固。模块A的任务场景中的一些安全配置比较明确，但另外一些安全配置则为不同的实现选项预留了选择空间，选手需根据行业最佳实践（在安全性、高可用性和可扩展性方面）选择合理安全方案，并尽最大努力实

现安全配置。选手应该熟悉Windows、linux等主流的网络安全设备和产品的安全配置和加固技术。

模块B: 包含网络安全事件响应、数字取证调查和应用程序安全。该模块需要选手根据企业所发现的安全事件，展开网络安全事件的调查、分析和取证工作，收集、保存、处理、分析和提供与计算机相关的证据，分析黑客的入侵行为，恢复被黑客破坏的文件。**B**模块主要考察选手网络安全事件应急处置能力、网络安全事件取证分析能力、应用程序的代码审计能力以及网络安全风险评估防控能力。

模块C: 为夺旗挑战赛（CTF），在一个有吸引力的环境中展示网络安全，并使安全专业人员能够在模拟的网络安全攻击场景中磨练自己的技能。本模块参赛选手作为攻击方，综合运用所掌握的网络安全攻击技能，开展网络渗透测试。在比赛期间，参赛队伍可以利用一系列网络安全攻击渗透工具综合分析、挖掘、渗透所提供的网络安全攻击靶场环境。靶场环境中预设了若干 Flag，每个 Flag 有固定的分值，选手要尽可能多的获取Flag 值。

（三）评判标准

1.竞赛试题配分

本项目各竞赛模块配分以及占总分的比例。

模块编号	模块名称	分数
A	企业基础设施安全	35%
B	网络安全事件响应、数字取证调查和应用安全	35%
C	CTF 夺旗-攻击	30%

总计	100%
----	------

2.成绩计算方式

评分过程采用千分制。

最终分数换算为百分制，各个评分项的分数应精确到小数点后两位，小数点后第三位数字采用四舍五入（如 1.055 计 1.06，1.054 计 1.05）。

3.评判方法

①评分阶段：

竞赛阶段	阶段名称	任务阶段	评分方式
模块A 权重35%	企业基础设施安全	任务1...N	裁判客观评分
模块B 权重35%	安全事件响应、网络安全数据取证、应用安全	任务1...N	机考评分
模块C 权重30%	CTF夺旗攻击	系统攻防演练	机考评分

②模块A评分规则

模块A总分为350分，分为N个任务，每道题的具体分值在赛题中标明；模块A企业基础设施安全部分评分由评分裁判按照评分标准客观评分；

③模块B评分规则

模块B总分为350分，分为N个任务，模块B安全事件响应、网络安全数据取证、应用安全等部分由系统自动评分和排名。

④模块C评分规则

模块C总分为300分，按照选手获得攻击“FLAG”的值得到相

应的分数,系统自动评分和排名。

4.成绩并列

当出现选手总成绩并列时,以 C 模块得分进行排序,如果C模块得分相同,以C模块最后一个flag提交时间排序。

三、竞赛细则

(一) 竞赛流程

1. 场次和工位抽签

根据大赛组委会要求,网络项目比赛共两天,分为三个模块。每个模块赛前选手依次抽取比赛工位,所有选手都要按照抽签工位参加两天三个模块的比赛。

2.日程安排

竞赛限定在 2 天内进行,赛项竞赛时间为 9 小时,具体安排如下:

赛前第 2 天 (C-2)				
时间	事项	参与人员	负责人	地点
07:00-24:00	工位布置和赛场搭建设备调试等	场地经理 会场布展人员 承接单位 设备设施支持单位	场地经理 赛项负责人	黄河会展中心 N3、 N4、N5 馆
08:00-12:00	裁判长及助理 裁判员 各地市代表团 报到	裁判长及助理 裁判员 领队及助理 选手等	后勤保障组	站场
13:00-13:20	出发前往赛场	领队及助理	后勤保障组	酒店
14:00-15:00	裁判长组织赛场现场查看	裁判长及助理 场地经理及助理 承接单位 布展服务单位	裁判长	黄河会展中心 N3、 N4、N5 馆

14:00-15:00	领队会	组委会 执委会 领队及助理 有关人员	组委会办公室	黄河会展中心 N3 馆 201 会议室
15:30	返回酒店	领队及助理	后勤保障组	会展中心乘车点
15:30-16:30	裁判长会及评分系统培训会	裁判长及助理 录分员 评分系统技术人员 监督仲裁组 组委会技术工作组 执委会技术和赛务 工作组	组委会办公室 执委会办公室	黄河会展中心 N3 馆 201 会议室
16:30-17:00	赛务对接会	裁判长及助理 场地经理及助理 组委会技术工作组 执委会技术和赛务 工作组	组委会办公室 技术和赛务工作 组 后勤保障组	黄河会展中心 N3 馆 201 会议室
17:30-18:30	晚餐	相关人员	后勤保障组	项目竞赛场地
赛前第 1 天 (C-1)				
时间	事项	参与人员	负责人	地点
6:40	早餐	全体人员	后勤保障组	酒店
7:20	出发前往赛场	裁判长及助理 裁判员 场地经理及助理 设备设施支持单位	后勤保障组	酒店
8:30-11:30	裁判培训会	裁判长及助理 裁判员 录分员 场地经理及助理	裁判长	项目竞赛场地
11:30-13:00	午餐	相关人员	后勤保障组	项目竞赛场地
12:00	出发前往赛场	领队及助理 选手 指导教师	后勤保障组	酒店
13:00-14:00	赛前说明会	裁判长及助理 裁判员 领队及助理 选手 指导教师	裁判长	项目竞赛场地
14:00-15:30	选手熟悉场地和设备设施	裁判长及助理 裁判员 领队及助理 选手 指导教师 场地经理及助理	裁判长	项目竞赛场地

		设备设施支持单位		
15:30-16:00	选手工具检查 查封	裁判长及助理 裁判员 选手 场地经理及助理	裁判长	项目竞赛场地
16:30	返回酒店	领队及助理 选手 指导教师	后勤保障组	会展中心乘车点
16:00-19:00 (具体赛项按实际情况调整)	场地设备等赛前检查、验封	裁判长及助理 裁判员 场地经理及助理 设备设施支持单位 监督仲裁组	裁判长	项目竞赛场地
17:30-18:30	晚餐	相关人员	后勤保障组	项目竞赛场地
20:00	返回酒店	裁判长及助理 裁判员 场地经理及助理 设备设施支持单位 监督仲裁组	后勤保障组	会展中心乘车点
比赛第1天(C1)				
时间	事项	参与人员	负责人	地点
6:40	早餐	全体人员	后勤保障组	酒店
7:20	出发前往赛场	裁判长及助理 裁判员 领队及助理 选手 指导教师 场地经理 技术支持单位	后勤保障组	酒店
7:30-8:00	场外安检	全体人员	后勤保障组	会展中心大厅
8:00	裁判就位	裁判 裁判长	裁判长	项目竞赛场地
8:00-8:15	选手抽签, 加密及入场	参赛选手 裁判 督导员	裁判长	项目竞赛场地
8:15 - 8:30	参赛选手就位宣读考场纪律, 设备检查、模块 A 赛题、U 盘发放	参赛选手 裁判 督导员	裁判长	项目竞赛场地
8:30 - 11:30	模块 A 竞赛	参赛选手	裁判长	项目竞赛场地

		裁判 督导员		
11:30 - 13:00	休息	参赛选手 裁判 督导员	后勤保障组	项目竞赛场地
13:00 - 17:30	模块 A 成绩评定	裁判 督导员	裁判长	项目竞赛场地
18:00-18:30	晚餐	相关人员	后勤保障组	项目竞赛场地
18:30-22:30	返回酒店	相关人员	后勤保障组	会展中心乘车点
比赛第 2 天 (C2)				
时间	事项	参与人员	负责人	地点
6:40	早餐	全体人员	后勤保障组	酒店
7:20	出发前往赛场	裁判长及助理 裁判员 领队及助理 选手 指导教师 场地经理 技术支持单位	后勤保障组	酒店
7:30-8: 00	场外安检	全体人员	后勤保障组	会展中心大厅
8:00	裁判就位	裁判 裁判长	裁判长 技术和赛务工作 组	项目竞赛场地
8:00 - 8:15	选手抽签, 加密及入场	参赛选手 裁判 督导员	裁判长	项目竞赛场地
8:15 - 8:30	参赛选手就位宣读考场纪律, 设备检查、模块 B 赛题	参赛选手 裁判 督导员	裁判长	项目竞赛场地
8:30 - 11:30	B 模块竞赛	参赛选手 裁判 督导员	裁判长	项目竞赛场地
11:30 - 13:00	休息	参赛选手 裁判 督导员	后勤保障组	
13:00 - 13:15	选手抽签, 加密及入场	参赛选手 裁判 督导员	裁判长	
13:15 - 13:30	参赛选手就位宣读考场纪律, 设备检查、模块 C 赛题	参赛选手 裁判 督导员	裁判长	

13:30-16:30	模块 C 竞赛	参赛选手 裁判 督导员	裁判长	
16: 30 - 18:00	成绩评定	裁判 督导员	裁判长	
18:30-22:30	返回酒店	相关人员	后勤保障组	会展中心乘车点
赛后第 1 天 (C+1)				
时间	事项	参与人员	负责人	地点
7:30	早餐	全体人员	后勤保障组	酒店
8:30	出发前往赛场	全体人员	后勤保障组	酒店-场馆
9:30-10:00	场外安检	全体人员	后勤保障组	场馆登录大厅
10:00-11:30	技术点评 公布成绩	裁判长及助理 裁判员 选手 场地经理及助理	裁判长	项目竞赛场地
11:30-13:00	午餐	相关人员	后勤保障组	项目竞赛场地
下午	闭幕式	嘉宾 获奖选手 获奖单位代表 工作人员 各代表团代表 新闻媒体 企业代表 参演志愿者	组委会办公室 执委会办公室 开闭幕式组	场馆登录大厅
下午	撤展（开始撤展时间以通知 为准）	场地经理 承接单位 布展服务单位 设备支持单位	执委会办公室	项目竞赛场地

最终竞赛时间安排以赛务手册为准。

（二）裁判员须知

本次竞赛设立裁判组，由 1 名裁判长及 1 名裁判长助理和若干裁判员组成。

1.裁判长

裁判长按照本项目技术文件，对裁判员进行培训和工作分工，带领裁判员对本项目比赛设备设施和现场布置情况进行检验；组

组织选手进行安全培训并熟悉赛场及设备，保障所有选手在比赛前掌握必备的安全知识和安全操作规范；比赛期间组织裁判员执裁，并按照相关要求和程序，处理项目内出现的问题；组织统计、汇总并及时录入大赛成绩等工作；赛后组织开展技术点评。裁判长应公平公正组织执裁工作，不参与评分。

2.裁判长助理

协助裁判长做好执裁各项组织工作；完成裁判长安排的相关工作。

3.裁判员

裁判员应服从本项目裁判长的工作安排，诚实、客观和公正执裁。

根据裁判员的相关工作经验以及赛前培训的情况，裁判长根据裁判员人数和工作量将裁判员分为三个组：加密裁判负责选手信息加密，现场裁判负责现场执裁并监督现场机考评分，评分裁判负责对选手提交的作品进行评判。

因为本赛项模块 A 由裁判人工客观评分，模块 B、C 由计算机自动评分，赛场内需进行选手信息加密，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。

所有加密结果密封袋的封条均需由相应加密裁判和监督人员签字。密封袋在监督人员监督下由加密裁判放置于保密室的保险柜中保存。

(三) 参赛选手须知

1.赛前准备

①参赛选手报到时需领取参赛证卡、参赛资料、参赛物料，报到完毕后提前前往赛场，熟悉场地。

②赛前 30 分钟，到指定检录口进行检录，由检录人员核实编号，开赛后迟到 15 分钟的选手视为自动放弃参赛。

③检录完毕，每位选手按照选手抽签工工位号到指定位置。可携带竞赛规定必备的工具、用具（如笔、草稿纸等）等。所有通讯、照相、摄像、磁盘等工具一律不得带入比赛现场。

2.竞赛实施

①在竞赛过程中，选手应遵守安全操作规程，接受裁判员的监督和警示，确保参赛选手人身安全及设备安全。

②竞赛过程中严禁交头接耳，也不能相互借用工具、仪器仪表。各参赛选手间不能走动、交谈。

③由裁判长统一告知选手比赛规则、时间和流程后，裁判长宣布比赛正式开始并计时。比赛过程中，选手若需休息、饮水或去洗手间，一律计算在操作时间内。

④选手进入赛场后，不得擅自离开赛场，因病或其他原因离开赛场或终止比赛，应向裁判示意，须经赛场裁判长同意，并在赛场记录表上签字确认后，方可离开赛场并在赛场工作人员指引下到达指定地点。

⑤因参赛选手个人误操作造成人身安全事故或设备故障时，裁判长有权中止选手竞赛。如非参赛选手个人因素出现的设备或

工具故障而无法继续竞赛时，参赛选手可提出更换设备或工具的要求，裁判长同意并更换后，参赛选手可继续参加竞赛，并给参赛选手补足所耽误的竞赛时间。选手自带设备和工具，赛场不负责更换。

⑥参赛选手如提前结束竞赛，应举手向裁判员报告，竞赛结束时间由裁判员进行记录。参赛选手结束竞赛后不得再进行任何操作，离场后也不得再进入赛场。

⑦裁判长在竞赛结束前 30 分钟、10 分钟进行竞赛剩余时间提醒。裁判长发布竞赛结束指令后，未完成任务的参赛选手应立即停止操作，不得以任何理由拖延竞赛时间，并按要求清理赛位。

⑧选手须按照程序提交比赛结果（任务书、报告），配合裁判做好赛场情况记录，并签字确认，裁判提出签名要求时，不得无故拒绝。

（四）工作人员须知

1. 场地经理

各竞赛项目设场地经理 1 名,负责组织相关工作人员做好竞赛设施设备、工具、材料落实及场地布置,参与赛务手册编制,配合裁判长做好技术工作文件编制、赛前准备和现场技术支持与后勤保障等工作。竞赛期间,场地经理应全程在竞赛区域值守。

2. 赛务保障人员

包括为各项目配各的竞赛联络员、技术负责人、录分员及其他赛务保障人员。按照相关要求,做好竞赛相关工作。

3.正式比赛期间，除裁判长外，任何人员不得主动接近选手及其工作区域，不得主动与选手接触与交流，选手有问题可向执裁裁判反映。

(五)成绩公布

最终成绩经复核无误，由裁判长会同裁判组签字确认后公布。实操比赛全部结束后 24 小时内公布最终成绩。

(六)技术违规处理

1.选手携带其他未经组委会认可的设备、工具、材料等参赛，取消比赛资格；

2.选手接收场外资料、软件、程序等，取消比赛资格；

3.在完成工作任务的过程中，因操作不当导致事故，扣总分 10%，情况严重者取消竞赛资格；

4.因违规操作损坏赛场提供的设备，污染赛场环境等严重不符合职业规范的行为，视情节扣总分 10%，情况严重者取消竞赛资格；

5.扰乱赛场秩序，干扰裁判员工作，视情节扣总分 10%，情况严重者取消竞赛资格；

6.裁判员严格遵守比赛规则，比赛期间不能与自己的选手有任何的单独接触行为，如果发现裁判为自己选手提供有违比赛公平的信息，一经查实取消该参赛队的比赛资格；

7.裁判评分期间，裁判员不能单独接触自己选手的电脑和环境，如发现裁判有违比赛规则的行为，选手本次比赛的成绩作废。

(七) 问题或争议处理

1.竞赛项目内解决

参赛选手、裁判员发现竞赛过程中存在问题或争议，应向裁判长反映。裁判长依据相关规定处理或组织比赛现场裁判员研究解决。处理意见需比赛现场全体裁判员表决，须获全体裁判员半数以上通过。最终处理意见应及时告知意见反映人。

2.监督仲裁组解决

本赛项在比赛过程中若出现有失公正或有关人员违规等现象，代表队领队可在比赛结束后 1 小时之内向监督仲裁工作组提出书面申诉。监督仲裁工作组在接到申诉后的 1 小时内组织复议，并及时反馈仲裁结果，经调查确认所反映情况属技术性问题的，仍交由竞赛项目内解决。属非技术性问题的，由监督仲裁组作最终裁决。各类问题或争议处理情况，由执委会填写《争议处理记录表》报监督仲裁工作组备案。没有书面申诉或超过 1 小时进行申诉的不予受理。

四、竞赛场地、设施设备等安排

(一) 赛场规格要求

- 1.本赛项场地总面积 299m²;
- 2.每组工位（2 人）面积 13 m²，工位间隔 50cm;
- 3.技术人员及裁判工作区域约 63 m²,配置必要的工作台椅、评分用的电脑及打印机，饮用水等。

竞赛的应用系统环境主要以 Windows 和 Linux 系统为主，涉及如下版本：

①物理机安装操作系统：微软 Windows 7(64 位)中文试用版或微软 Windows 10(64 位)中文试用版。

②虚拟机安装操作系统：

Windows 系统（试用版）：Windows XP、Windows 7、Windows 10、Windows Server2003 及以上版本（根据命题实际确定）。

Linux 系统：Ubuntu、Debian、CentOS（具体版本根据命题实际确定）。

③其他主要应用软件为（实际竞赛环境可能不仅限于以下软件）：

VMware workstation 12 pro 及以上版本免费版

Putty 0.67 及以上版本

Chrome 浏览器 62.0 及以上版本

RealVNC 客户端 4.6 及以上版本

2.裁判使用设备和工具

裁判使用设备和工具清单表

序号	设备名称	型号（备注）	单位	数量
1	PC	CPU 主频 $\geq$ 2.6GHZ, $\geq$ 四核四线程；内存 $\geq$ 8G；硬盘 $\geq$ 240G；支持硬件虚拟化。 分辨：1920*1080 及以上 标配键盘鼠标； 显示器要求宽屏， $\geq$ 21 英寸； 安装 Office、PDF 阅读器、谷歌浏览器	台	6
2	打印机	黑色打印	台	1

3.选手自备的设备和工具

网络安全项目无需选手自带工具。

4.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，选手禁止携带任何带有存储功能电子产品进入赛场，另外还要遵循如下规定：

任何储存液体、气体的压力容器；

任何有腐蚀性、放射性的化学物品；

任何易燃、易爆物品；

任何有毒、有害物品；

任何可能危及安全问题的物品；

任何影响竞赛公平性的物品。

（四）竞赛服务平台

该赛项结合企业职业岗位对人才培养需求，涉及的信息网络安全工程在设计、组建过程中，主要有以下 8 项国家职业标准，参赛选手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	GA/T 1389-2017	《信息安全技术网络安全等级保护定级指南》
2	GB 17859-1999	《计算机信息系统安全保护等级划分准则》
3	GB/T 20271-2006	《信息安全技术信息系统通用安全技术要求》
4	GB/T 20270-2006	《信息安全技术网络基础安全技术要求》
5	GB/T 20272-2006	《信息安全技术操作系统安全技术要求》
6	GB/T 20273-2006	《信息安全技术数据库管理系统安全技术要求》
7	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》
8	GB/T 20269-2006	《信息安全技术信息系统安全管理要求》

1.硬件环境

序号	设备名称	数量	设备要求
1	网络安全竞赛平台	1	<p>1. 能完成基础设施设置、安全加固、安全事件响应、网络安全数据取证、应用安全、CTF 夺旗攻击、CTF 夺旗防御等知识、技能内容竞赛环境实现，能有效支持 300 人规模，具备基于本规程竞赛内容同一场景集中答题环境。</p> <p>2. 标配 2 个千兆以太网口，Intel 处理器，大于等于 16G 内存，双 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；阶段间无需人工切换，系统自动处理；</p> <p>模块 B、C 全过程自动评判，支持竞赛过程图像元素上传，支持加密文件格式导入，内容包含不限于用户信息、任务、试卷、场景、答案、虚拟资源等。支持 KVM 虚拟机及 Docker 容器，支持多种虚拟机操作系统模板 windows/linux，不限于 img、qcow2 格式虚拟镜像文件。每个战队配置完全独立的靶机资源，队员可修复本队靶机漏洞提交静态 FLAG 得分、提交其他队伍靶机内动态 FLAG 得分，系统支持设置自动检测程序，检测队伍靶机漏洞是否修复。</p>
2	WEB 应用防火墙	1 台	支持透明模式、支持 trunk、支持 80 端口内容过滤、黑白名单、其他非 80 端口数据二层放行
3	UPS	1 台	最低支持 1 台服务器 5 分钟以上供电
4	交换机	2 台	24 口三层交换机

五、安全健康要求

(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,例如:ESD(静电放电),静电放电无害环境下的设备用途,安全使用及储存。
- 4.参赛选手应保证设备和信息完整及安全。

(二) 赛事安全要求

- 1.禁止选手及所有参加赛事的人员携带任何有毒有害物品进入竞赛现场。
- 2.承办单位应在设置专门的安全防卫组,负责竞赛期间健康和安 全事务。主要包括检查竞赛场地、与会人员居住地、车辆交通及其周围环 境的安全防卫;制定紧急应对方案;监督与会人员食品安全与卫生;分析和处理安全突发事件等工作。
- 3.赛场须配备相应医疗人员和急救人员,并备有相应急救设施。

(三) 绿色环保要求

- 1.赛场严格遵守我国环境保护法。
- 2.赛场所有废弃物应有效分类并处理,尽可能地回收利用。
- 3.竞赛相关人员,要注意保持环境整洁卫生,垃圾集中存放。

4. 每场竞赛结束后，选手要做到工完场清，赛场保洁人员要保障赛场整体的环境卫生，体现安全、整洁、有序。

六、其他

经大赛组委会允许的赞助商、负责宣传的媒体记者和其他参观人员，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、烦扰选手的正常比赛。与大赛相关的赛题、评分细则、技术文件等均有著作权保护，未经许可不得它用。