全国职业院校技能大赛
赛项规程

一、赛项名称

赛项编号：ZZ-2021029

赛项名称：网络安全

英文名称：Cyber Security

赛项组别：中职组

赛项归属产业：信息技术类

二、竞赛目的

为检验中职学校网络信息安全人才培养成效，促进网络信息安全专业教学改革，培养大批既满足国家网络安全战略需要有具备世界水平的优秀技能人才，在社会上营造“技能改变命运、匠心成就人生”的崇尚技能的氛围，国家教育部联合多部委联合特举办本赛项。

（一）检验教学成效

竞赛内容涵盖了网络信息安全行业企业岗位对学生职业技能的最新要求，竞赛过程为完整工作任务的具体实施，竞赛评价标准符合业界项目验收和交付标准。通过竞赛，能够很好地反映出中职学校学生所培养的技能和用人单位岗位要求的匹配程度，从而检验网络信息安全专业教学成效，展现信息安全人才培养成果。

（二）促进教学改革

竞赛内容源自企业真实的项目和工作任务，其内容和要求直接反映了网络信息安全技术岗位要求，引导学校将专业与职业岗位对接、

课程内容与职业标准对接、教学过程与工作过程对接、学历证书与职业资格证书对接。通过竞赛，引导中职学校将企业完整的工作任务转化成教学内容；将传统重讲授轻实践的教学模式转向“做中学、做中教”项目案例教学；将职业资格能力作为专业的核心能力进行培养，从而提高人才培养的针对性和有效性。

（三）向世界高水平看齐

本赛项紧跟网络信息安全行业的发展趋势，瞄准国际网络安全技术发展水平，竞赛内容融入行业发展的最新技术。引领广大中职学校不断在新的更高的起点上培养国家需要、国际水准的网络信息安全技能人才，服务国家战略，建设网络强国。

（四）营造崇尚技能的社会氛围

技能人才是人才队伍的重要组成部分，良好的社会氛围是技能人才成长成才的环境和基础，关系到技能人才队伍的长远发展。通过竞赛宣传，引导全社会尊重、重视、关心技能人才的培养和成长，让尊重劳动、尊重技术、尊重创新成为社会共识。通过竞赛，表彰一批优秀的年轻的技能人才，增强他们的自豪感、获得感，在全国上下营造“技能改变命运、匠心成就人生”的崇尚技能的氛围，激励广大青年走技能成才、技能报国之路。

三、竞赛内容

3.1 标准规范

主要考核参赛选手网络系统安全策略部署、信息保护、网络安全运维管理、网络安全事件应急响应、网络安全数据取证、应用安全、

代码审计等综合实践能力，具体包括：

项目	
1	**工作组织和管理**
	个人（选手）需了解和理解： • 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。
	个人（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 • 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	**通讯和人际沟通技巧**
	个人（选手）需了解和理解：

	• 倾听是很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。
	个人（选手）应具备的能力： • 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**
	个人（选手）需了解和理解： • 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。
	个人（选手）应具备的能力：

	• 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**
	个人（选手）需了解和理解： • 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。
	个人（选手）应具备的能力： • 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**
	个人（选手）需了解和理解： • 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。
	个人（选手）应具备的能力： • 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。
6	**分析**
	个人（选手）需了解和理解： • 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。
	个人（选手）应具备的能力： • 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**
	个人（选手）需了解和理解： • 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。
	个人（选手）应具备的能力： • 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**
	个人（选手）需了解和理解： • 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。
	个人（选手）应具备的能力： • 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。

3.2 竞赛分值权重和时间安排

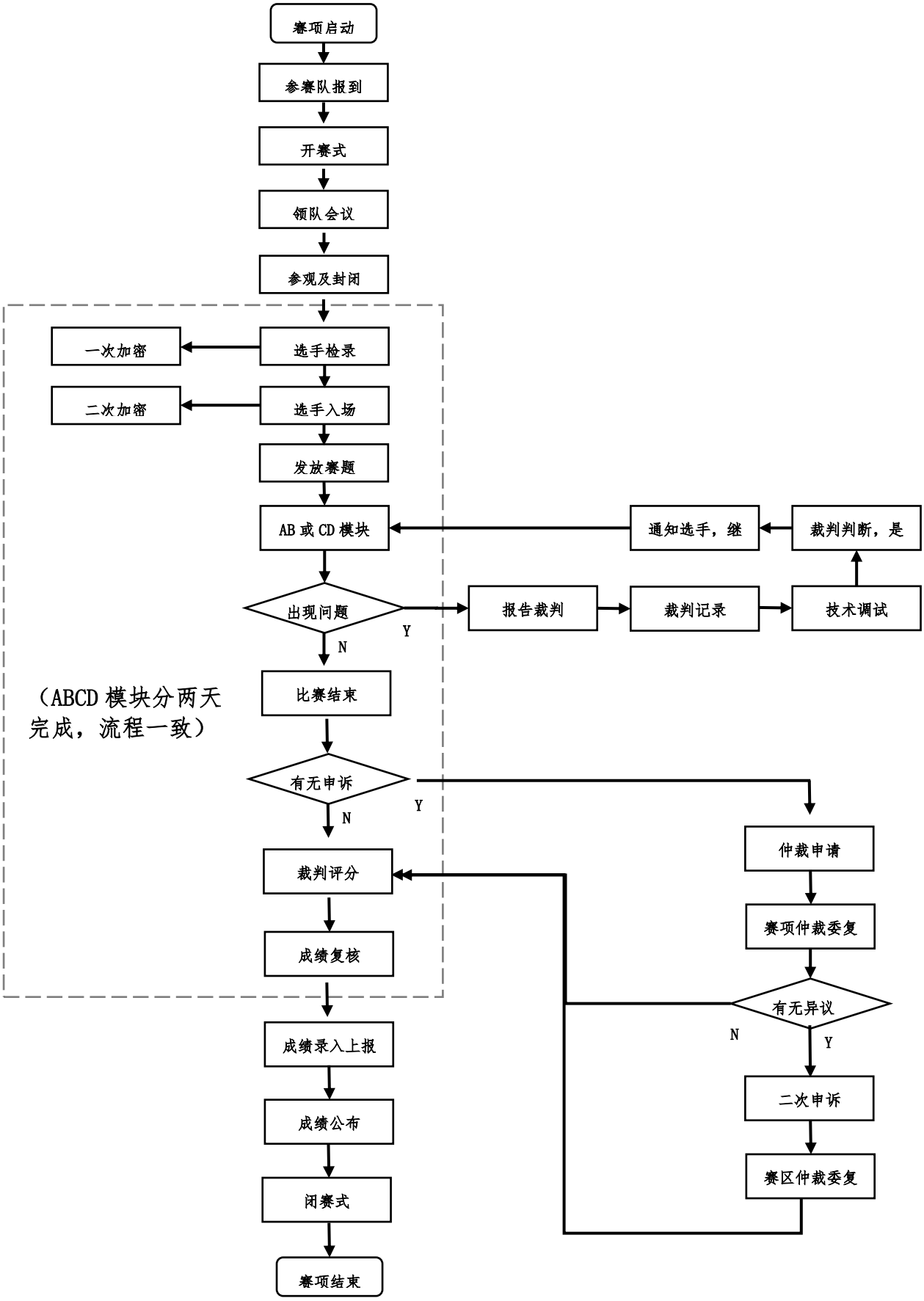
模块编号	模块名称	竞赛时间（小时）	分数权值
A	基础设施设置与安全加固	3	20%
B	网络安全事件响应、数字取证调查和应用安全		40%
C	CTF 夺旗-攻击	3	20%
D	CTF 夺旗-防御		20%
总计		6	100%

四、竞赛方式

本赛项为团体赛，以省（自治区、直辖市、新疆生产建设兵团）为单位组队，各地限额推荐 1 支队伍参赛，每个参赛队由 2 名选手组成，不得跨校组队，每个参赛队限报 2 名指导教师。

五、竞赛流程

（一）竞赛流程图


赛项启动
参赛队报到
开赛式
领队会议
参观及封闭
选手检录
一次加密
选手入场
二次加密
发放赛题
AB 或 CD 模块
通知选手，继
裁判判断，是
出现问题
Y
报告裁判
裁判记录
技术调试
N
比赛结束
（ABCD 模块分两天完成，流程一致）
有无申诉
Y
N
仲裁申请
裁判评分
赛项仲裁委复
成绩复核
有无异议
N
Y
成绩录入上报
二次申诉
成绩公布
赛区仲裁委复
闭赛式
赛项结束

（二）竞赛时间表

竞赛在 2 天内进行，具体安排如下：

日期	时间	事项	参加人员	地点
赛前 2日	20:00前	专家组、裁判组、监督仲裁组报到	工作人员	住宿酒店
赛前 1 日	09:00-12:00	参赛队报到，安排住宿，领取资料	工作人员、参赛队	住宿酒店
	14:00-15:00	开赛式	工作人员、参赛队	会议室
	15:00-15:30	领队会	各参赛队领队、裁判长、监督仲裁组	会议室
	15:30-16:00	参观赛场	各参赛队领队	竞赛场地
	16:00	返回酒店	各参赛队领队	竞赛场地
	16:00	检查、封闭赛场	裁判组、监督仲裁组	竞赛场地
	16:00-18:00	裁判工作会议	裁判组、监督仲裁组	会议室
竞赛第一天	07:30	裁判就位	裁判组、监督仲裁组	竞赛场地
	07:30-08:00	选手抽签，一次加密	参赛选手、裁判组、监督仲裁组	竞赛场地
	08:00-08:30	选手抽签，二次加密及入场	参赛选手、裁判组、监督仲裁组	竞赛场地
	08:30-08:40	参赛选手就位，宣读考场纪律	参赛选手、裁判组、监督仲裁组	竞赛场地
	08:40-09:00	设备检查、模块 A、模块 B 赛题发放	参赛选手、裁判组、监督仲裁组	竞赛场地
	09:00-12：00	模块 A、B 竞赛	参赛选手、裁判组、	竞赛场地

			监督仲裁组	
	12:00	A、B 模块比赛结束	参赛选手、领队、指导教师	住宿酒店
	12：00-18：00	成绩评定、核查、解密、确认	裁判组、监督仲裁组	竞赛场地
竞赛第二天	07:30	裁判就位	裁判组、监督仲裁组	竞赛场地
	07:30-08:00	选手抽签，一次加密	参赛选手、裁判组、监督仲裁组	竞赛场地
	08:00-08:30	选手抽签，二次加密及入场	参赛选手、裁判组、监督仲裁组	竞赛场地
	08:30-08:40	参赛选手就位，宣读考场纪律	参赛选手、裁判组、监督仲裁组	竞赛场地
	08:40-09:00	设备检查、模块 C、D 模块赛题发放	参赛选手、裁判组、监督仲裁组	竞赛场地
	09:00-12：00	模块 C、D 竞赛	参赛选手、裁判组、监督仲裁组	竞赛场地
	12:00	C、D 模块比赛结束	参赛选手、领队、指导教师	住宿酒店
	12：00-18：00	成绩评定、核查、解密、确认	裁判组、监督仲裁组	竞赛场地
	18:00-24:00	成绩公布，成绩报送	裁判组、监督仲裁组	竞赛场地
赛后 1 日	9：00-11：00	闭幕式	领导、嘉宾、裁判组、各参赛队	会议室

六、竞赛赛卷

（一）本赛项赛卷公开，竞赛赛卷距国赛开始日前一个月公开。

（二）本赛项通过大赛指定的网络信息发布平台（http://www.chinaskills-jsw.org）公布竞赛赛卷。

赛卷样题见附件一。

七、竞赛规则

（一）报名资格

参赛选手须为 2021 年度在籍全日制中等职业学校学生；五年制全日制高职一至三年级（含三年级）在籍学生可参加竞赛。参赛选手不限性别，年龄须不超过 21 周岁，年龄计算的截止时间以 2020 年 5 月 1 日为准。

（二）竞赛工位通过抽签决定，竞赛期间参赛选手不得离开竞赛工位。

（三）竞赛所需的硬件设备、系统软件和辅助工具由组委会统一安排，参赛选手不得自带硬件设备、软件、移动存储、辅助工具、移动通信等进入竞赛现场。

（四）参赛选手自行决定工作程序和时间安排。

（五）参赛选手在赛前 20 分钟进入竞赛工位并领取竞赛任务，竞赛正式开始后方可展开相关工作。

（六）竞赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和警示。若因选手因素造成设备故障或损坏，无法继续竞赛，裁判长有权决定终止该队竞赛；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。

（七）竞赛结束（或提前完成）后，参赛选手起立，在确认后不得再进行任何操作，按顺序离场。

（八）最终竞赛成绩经复核无误及裁判长、监督长签字确认后，在指定地点，以纸质形式在指定点向全体参赛队进行提前公布，各参赛队无异议后在闭赛式上予以宣布。

（九）本赛项各参赛队最终成绩由承办单位信息员录入赛务管理系统。承办单位信息员对成绩数据审核后，将赛务系统中录入的成绩导出打印，经赛项裁判长审核无误后签字。承办单位信息员将裁判长确认的电子版赛项成绩信息上传赛务管理系统，同时将裁判长签字的纸质打印成绩单报送大赛执委会。

（十）赛项结束后专家工作组根据裁判判分情况，分析参赛选手在竞赛过程中对各个知识点、技术的掌握程度，并将分析报告报备大赛执委会办公室，执委会办公室根据实际情况适时公布。

（十一）赛项每个竞赛环节裁判评分的原始材料和最终成绩等结果性材料经监督组人员和裁判长签字后装袋密封留档，并由赛项承办院校封存，委派专人妥善保管。

八、竞赛环境

1.竞赛场地。竞赛场地的配备必须符合疫情防疫要求，竞赛现场设置竞赛区、裁判区、服务区、技术支持区。现场保证良好的采光、照明和良好通风；提供稳定的水、电和供电应急设备，提供足够的干粉灭火器材。同时提供所有指导教师休息室 1 间。

2.竞赛设备。竞赛设备由执委会和承办校负责提供和保障，竞赛区按照参赛队数量准备竞赛所需的软硬件平台，为参赛队提供标准竞赛设备。

3.竞赛工位。工位间距和场地空间必须符合疫情防疫要求，竞赛现场各个工作区配备单相 220V/3A 以上交流电源。每个竞赛工位上标明编号并用隔离带隔离，确保参赛队之间互不干扰，每个竞赛工位配备 2 把工作椅（凳）。

4.技术支持区为技术支持人员的工作场地，为参赛选手竞赛提供网络环境部署和网络安全防范。

5.服务区提供医疗等服务保障，并用隔离带隔离。

6.竞赛工位隔离和抗干扰。竞赛工位之间标有隔离线。

九、技术规范

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》

十、技术平台

（一）竞赛器材

序号	设备名称	数量	设备要求
1	网络安全竞赛平台	1	磐云 PY-B7v2(北京中科磐云科技有限公司) 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。 2. 标配 2 个千兆以太口，Intel 处理器，大于等于 16G 内存，SSD +SATA 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；提供单兵闯关、分组混战等实际对战模式，阶段间无需人工切换，系统自动处理；提供超过 20 种不同级别 70 个的攻防场景；模块 B、C 全过程自动评判，支持竞赛过程图像元素上传，排名判定策略大于等于 12 种；自定义动画态势展示，成绩详细分析;支持监控异常虚拟机,同时检测 FTP、HTTP、ICMP、SMTP、SSH、TCP 和 UDP 协议，服务端口支持在有效范围内的服务端口；支持全程加密，

			支持加密文件导入，加密方式为非对称加密，设备能随机生成密码。
2	PC 机	2	CPU 主频>=2.8GHZ,>=四核四线程；内存>=8G；硬盘>=500G；支持硬件虚拟化。

（二）软件技术平台：

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

Python/Python3 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

360 压缩 4.0 及以上版本

JDK（Java Development Kit）7.0 及以上版本

十一、成绩评定

（一）裁判工作原则

赛前建立健全裁判组。裁判组为裁判长负责制。

本赛项拟设裁判 21 名。其中裁判长 1 名，副裁判长 1 名，现场裁判 8 名，评分裁判 8 名，加密裁判 3 名。

因为本赛项模块 A、D 由裁判人工客观评分，模块 B、C 由计算机自动评分，赛场内需进行两次加密，提交作品需进行三次加密。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：对参赛选手提交作品进行第三次加密，将加密后的成果，交由裁判长组织评分裁判进行评分。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。

（二）裁判评分方法

现场裁判组监督现场机考评分，评分裁判负责参赛选手提交作品评分，裁判长负责竞赛全过程。

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。

（三）成绩产生办法

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 20%	基础设施设置、安全加固	任务 1...N	裁判客观评分
模块 B 权重 40%	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 20%	CTF 夺旗攻击	系统攻防演练	机考评分
模块 D 权重 20%	CTF 夺旗防御	系统攻防演练	裁判客观评分

2.模块 A、模块 B 评分规则

模块 A 总分为 20 分，考核选手基础设施设置、安全加固，由评分裁判客观评分；

模块 B 总分为 40 分，考核选手安全事件响应、网络安全数据取证、应用安全等，分为 10 个任务，每道题的具体分值在赛题中标明，由系统自动评分和排名，对外公开显示。

3.模块 C、模块 D 评分规则

模块 C 总分为 20 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，对外公开显示。

模块 D 总分为 20 分，按照选手答题内容，由评分裁判进行客观评分。

选手在答题过程中不得违反竞赛试题要求答题，不得以违规形式获取得分，不得违规攻击裁判服务器、网关、系统服务器等非靶机目标，如检测选手有违规攻击行为，警告一次后若继续攻击，判令该队终止竞赛，清离出场。

（四）裁判人员具体要求

序号	专业技术方向	知识能力要求	执裁、教学、工作经历	专业技术职称（职业资格等级）	人数
1	计算机网络技术、信息安全、网络安全、通信工程	熟悉计算机网络技术、信息安全技术	从事计算机网络技术、信息安全专业教学或相关比赛执裁经验	正高	1
2	计算机网络技术、信息安全、网络安全、通信工程	熟悉计算机网络技术、信息安全技术	从事计算机网络技术、信息安全专业教学或相关比赛执裁经验	副高（国家一级职业资格证）	20
裁判总人数	21 人				

十二、奖项设定

本赛项为团队赛，依照实际参赛队数量确定奖项：一等奖占参赛队总数的 10%，二等奖占参赛队总数的 20%，三等奖占参赛队总数的 30%。

获得一等奖参赛队的指导教师获“优秀指导教师奖”称号，授予荣誉证书。

十三、赛场预案

为保障赛项顺利进行，避免竞赛过程中不可控但可能出现的紧急情况，赛项预案由赛项可靠性设计、故障的应急处理方案两部分组成。

（一）赛项可靠性设计

1.电力系统可靠性设计

供电负荷匹配电力要求，防止电子设备运行过程中过载导致火灾隐患或电力中断；提供三项电源接地保证，杜绝运行过程中静电可能导致设备重启、短路、漏电等安全威胁；布线强弱电分离，防止发生干扰；各区域供电保障独立，相互不干扰。

2.弱电系统可靠性设计

弱电系统必须保证良好的运行状态，系统应具备长期和稳定的工作能力，遇到突发状况时应存在快速解决方法，保证系统可靠运行。弱电系统应与电力系统隔离部署，防止干扰造成故障。

3.网络设备可靠性设计

网络设备必须要运行稳定，满足带宽要求，预留端口备份，通信线缆、设备预留备份，具备故障快速恢复机制，提供必要的冗余备份设计。

4.攻防平台可靠性设计

平台必须支持集群功能，在大规模流量下支持负载分担，同时可为竞赛数据提供备份、回退机制。具备冗余备份机制，在最短时间内恢复故障问题。平台应提供访问控制机制，具备防攻击手段，保障平台运行稳定。

5.PC 可靠性设计

PC 的部署必须保证良好的运行状态，遇到突发状况时应存在快速解决方法，保证系统可靠运行。系统规格必须满足要求，保证良好的性能和稳定的运行。

（二）故障的应急处理方案

1.参赛选手 PC 故障

如参赛选手 PC 遇到故障，先判断其为硬件故障还是软件故障。软件故障或出现卡顿现象则对 PC 进行重启，因 PC 配备还原卡，可将系统恢复至初始状态，故障恢复时间约 30 秒；硬件故障经过现场裁判允许后更换备用机，故障恢复时间约 1 分钟。键盘、鼠标故障及时更换，恢复时间约 1-3 分钟。不会对学生成绩产生影响。

2.竞赛工位线缆连接故障

竞赛工位如遇到网络连接问题，现场裁判判定线缆物理连接问题，非选手设置操作导致，应及时更换备用线缆，故障恢复时间约 30 秒；竞赛工位两条以上网线物理故障，经现场裁判允许为其更换竞赛工位，故障恢复时间约 3-5 分钟。

3.竞赛工位电力故障

如遇竞赛工位电力故障，经裁判长允许更换备用工位。故障恢复时间 3-5 分钟。

4.网络设备交换机故障

更换备用交换机，故障恢复时间约 5-10 分钟；跳线线缆故障及时更换备用线缆（光纤及网线），故障恢复时间约 3-5 分钟。

5.攻防平台集群故障

服务器集群主设备故障，启用备用集群设备，数据互备份，集群恢复时间约 5-10 分钟。服务器集群从设备故障，更换备用设备，恢复时间约 5-10 分钟。成绩实时保存，不会对学生成绩产生影响。

6.WEB 应用防火墙故障

如遇 WAF 设备故障，影响访问，取消防护策略或取消 WAF 设备连接，故障恢复时间约 1-3 分钟。

7.服务器区供电问题

若服务器区发生供电问题，UPS 电源可支持约 20-30 分钟。

十四、赛项安全

赛事安全是一切工作顺利开展的先决条件，是本赛项筹备和运行工作必须考虑的核心问题。

（一）组织机构

赛项组织专门机构负责赛区内赛项的安全工作，建立公安、消防、司法行政、交通、卫生、食品、质检等相关部门协调机制保证竞赛安全。制定相应安全管理的规范、流程和突发事件应急预案，及时处置突发事件，全过程保证竞赛筹备和实施工作安全。

（二）赛项设计

1.竞赛内容涉及的器材、设备应符合国家有关安全规定。赛项专家组应充分考虑竞赛内容和所用器材、耗材可能存在的危险因素，通过完善设计规避风险，采取有效防范措施保证选手备赛和竞赛安全。危险提示和防范措施应在赛项技术文件中加以明确。

2.赛项技术文件应包含国家（或行业）有关职业岗位安全的规范、条例和资格证书要求等内容。

3.赛前对本赛项全体裁判员进行裁判培训和安全培训，对服务人员进行安全培训。源于实际生产过程的赛项，须根据《中华人民共和国劳动法》等法律法规，建立完善的安全事故防范制度，并在赛前对选手进行培训，避免发生人身伤害事故。

（三）竞赛环境

1.环境安全保障

赛场组织与管理员应制定防疫预案、安保须知、安全隐患规避方法及突发事件预案，设立紧急疏散路线及通道等，确保竞赛期间所有

进入竞赛地点的车辆、人员需凭证入内；严禁携带易燃易爆物、管制刀具等危险品及竞赛严令禁止的其他物品进入场地；对于紧急发生的拥挤、踩踏、地震、火灾等进行紧急有效的处置。

2.信息安全保障

安装 UPS：采用 UPS 防止现场因突然断电导致的系统数据丢失。后备时间：2 小时；输出电压：230V±5%V；市电采用双路供电。

3.操作安全保障

赛前要对选手进行计算机、网络设备、工具等操作的安全培训，进行安全操作的宣讲，确认每个队员能够安全操作设备后方可进行竞赛。裁判员在竞赛前，宣读安全注意事项，强调用火、用电安全规则。整个大赛过程邀请当地公安系统、卫生系统和保险系统协助支持。参赛选手旅途及竞赛过程中的安全保障由各省市负责。

4.赛项执委会须在赛前组织专人对竞赛现场、住宿场所和交通保障进行考察，并对安全工作提出明确要求。赛场的布置，赛场内的器材、设备，应符合国家有关安全规定。如有必要，也可进行赛场仿真模拟测试，以发现可能出现的问题。承办单位赛前须按照要求排除安全隐患。

5.赛场周围要设立警戒线，防止无关人员进入发生意外事件。竞赛现场内应参照相关职业岗位的要求为选手提供必要的劳动保护。在具有危险性的操作环节，裁判员要严防选手出现错误操作。

6.承办单位应提供保证应急预案实施的条件。对于内容涉及高空作业、可能有坠物、大用电量、易发生火灾等情况的赛项，必须明确制度和预案，并配备急救人员与设施。

7.赛项组织部门须会同承办单位制定开放赛场和体验区的人员

疏导方案。赛场环境中存在人员密集、车流人流交错的区域，除了设置齐全的指示标志外，须增加引导人员，并开辟备用通道。

8.大赛期间，赛项承办单位须在赛场管理的关键岗位，增加力量，建立安全管理日志。

9.参赛选手进入赛位、赛事裁判工作人员进入工作场所，严禁携带通讯、摄录设备，禁止携带记录用具。如确有需要，由赛场统一配置、统一管理。赛项可根据需要配置安检设备对进入赛场重要部位的人员进行安检。

（四）生活条件

1.竞赛期间原则上由执委会委托赛事承办单位统一安排参赛选手和指导教师食宿。承办单位须尊重少数民族的信仰及文化，根据国家相关的民族政策，安排好少数民族选手和教师的饮食起居。

2.竞赛期间安排的住宿地应具有宾馆/住宿经营许可资质。以学校宿舍作为住宿地的，大赛期间的住宿、卫生、饮食安全等由赛项组织部门和提供宿舍的学校共同负责。

3.各赛项的安全管理，除了采取必要的安全隔离措施外，应严格遵守国家相关法律法规，保护个人隐私和人身自由。

（五）防疫防控要求

按照相关部门的关于防疫防控的统一要求执行。

（六）组队责任

1.各省、自治区、直辖市在组织参赛时，须安排为参赛选手购买大赛期间的人身意外伤害保险。

2.各省、自治区、直辖市须制定相关管理制度，并对所有选手、指导教师进行安全教育。

3.各参赛选手领队须加强参赛人员的安全管理，实现与赛场安全管理的对接。

（七）应急处理

竞赛期间发生意外事故，发现者应第一时间报告赛项组织部门，同时采取措施避免事态扩大。赛项组织部门应立即启动预案予以解决并向赛区执委会报告。出现重大安全问题的赛项可以停赛，是否停赛由赛区组委会决定。事后，赛区执委会应向大赛执委会报告详细情况。

（八）处罚措施

1.赛项出现重大安全事故的，停止承办单位的赛项承办资格。

2.因参赛选手原因造成重大安全事故的，取消其参赛资格。

3.参赛选手有发生重大安全事故隐患，经赛场工作人员提示、警告无效的，可取消其继续竞赛的资格。

4.赛事工作人员违规的，按照相应的制度追究责任。情节恶劣并造成重大安全事故的，由司法机关追究相应法律责任。

十五、竞赛须知

（一）参赛队须知

1.参赛队应该参加赛项承办单位组织的闭赛式等各项赛事活动。

2.在赛事期间，领队及参赛队其他成员不得私自接触裁判，凡发现有弄虚作假者，取消其参赛资格，成绩无效。

3.所有参赛人员须按照赛项规程要求按照完成赛项评价工作。

4.对于有碍竞赛公正和竞赛正常进行的参赛队，视其情节轻重，按照相关管理办法给予警告、取消竞赛成绩、通报批评等处理。

（二）参赛领队须知

1.由省、自治区、直辖市、新疆生产建设兵团教育行政部门确定

赛项领队1人，赛项领队应该由参赛院校中层以上管理人员或教育行政部门人员担任，熟悉赛项流程，具备管理与组织协调能力。

2.领队应按时参加赛前领队会议，不得无故缺席。

3.领队负责组织本省参赛队参加各项赛事活动。

4.领队应积极做好本省参赛队的服务工作，协调各参赛队与赛项组织机构、承办院校的对接，按照防疫要求做好团队各项防疫工作。

5.参赛队认为存在不符合竞赛规定的设备、工具、软件，有失公正的评判、奖励，以及工作人员的违规行为等情况时，须由领队向赛项仲裁组提交书面申诉材料。各参赛队领队应带头服从和执行申诉的最终仲裁结果，并要求指导教师、选手服从和执行。

（三）指导教师须知

1.指导教师应该根据专业教学计划和赛项规程合理制定训练方案，认真指导选手训练，培养选手的综合职业能力和良好的职业素养，克服功利化思想，避免为赛而学、以赛代学。

2.指导老师应及时查看大赛专用网页有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、技术规范和赛场要求，指导选手做好赛前的一切技术准备和竞赛准备。

3.指导教师应该根据赛项规程要求做好参赛选手保险办理工作，按照防疫要求做好团队防疫工作，并积极做好选手的安全教育。

4.指导教师参加赛项观摩等活动，不得违反赛项规定进入赛场，干扰竞赛正常进行。

（四）参赛选手须知

1.各参赛选手要按照防疫要求做好个人和团队防疫工作，发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，

取消参赛资格，名次无效。

2.参赛选手应按有关要求如实填报个人信息，否则取消竞赛资格。

3.参赛选手应按照规定时间抵达赛场，凭统一印制的参赛证、有效身份证件检录，按要求入场，不得迟到早退。请勿携带任何电子设备及其他资料、用品进入赛场。

4.参加选手应认真学习领会本次竞赛相关文件，自觉遵守大赛纪律，服从指挥，听从安排，文明参赛。

5.参赛选手应增强角色意识，科学合理做好时间分配。

6.参赛选手应按有关要求在指定位置就坐。

7.参赛选手须在确认竞赛内容和现场设备等无误后开始竞赛。在竞赛过程中，确因计算机软件或硬件故障，致使操作无法继续的，经项目裁判长确认，予以启用备用计算机。

8.各参赛选手必须按规范要求操作竞赛设备。一旦出现较严重的安全事故，经总裁判长批准后将立即取消其参赛资格。

9.参赛选手需详细阅读赛题中竞赛文档命名的要求，不得在提交的竞赛文档中标识出任何关于参赛选手地名、校名、姓名、参赛编号等信息，否则取消竞赛成绩。

10.竞赛时间终了，选手应全体起立，结束操作，将资料和工具整齐摆放在操作平台上，经工作人员清点后可离开赛场。离开赛场时不得带走任何资料。

11.在竞赛期间，未经执委会批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

（五）工作人员须知

1.树立服务观念，一切为选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，在赛项组织部门的领导下，按照各自职责分工和要求认真做好岗位工作。

2.所有工作人员必须佩带证件，忠于职守，秉公办理，保守秘密。

3.注意文明礼貌，保持良好形象，熟悉赛项指南。

4.自觉遵守赛项纪律和规则，服从调配和分工，确保竞赛工作的顺利进行。

5.提前 30 分钟到达赛场，严守工作岗位，不迟到，不早退，不得无故离岗，特殊情况需向工作组组长请假。

6.熟悉竞赛规程，严格按照工作程序和有关规定办事，遇突发事件，按照应急预案，组织指挥人员疏散，确保人员安全。

7.工作人员在竞赛中若有舞弊行为，立即撤销其工作资格，并严肃处理。

8.保持通讯畅通，服从统一领导，严格遵守竞赛纪律，加强协作配合，提高工作效率。

十六、申诉与仲裁

各参赛队对不符合大赛和赛项规程规定的仪器、设备、工装、材料、物件、计算机软硬件、竞赛使用工具、用品，竞赛执裁、赛场管理，以及工作人员的不规范行为等，可向赛项仲裁组提出申诉。申诉主体为参赛队领队。参赛队领队可在当天竞赛结束后（选手赛场竞赛内容全部完成）2 小时之内向仲裁组提出书面申诉，超过时效不在处理。

书面申诉应对申诉事件的现象、发生时间、涉及人员、申诉依据

等进行充分、实事求是的叙述，并由领队亲笔签名。非书面申诉不予受理。

赛项仲裁工作组在接到申诉报告后的2小时内组织复议，并及时将复议结果以书面形式告知申诉方。申诉方对复议结果仍有异议，可由省（市）领队向赛区仲裁委员会提出申诉。赛区仲裁委员会的仲裁结果为最终结果。

仲裁结果由申诉人签收，不能代收，如在约定时间和地点申诉人离开，视为自行放弃申诉。

申诉方可随时提出放弃申诉，不得以任何理由采取过激行为扰乱赛场秩序。

十七、竞赛观摩

本赛项将提供公开观摩区，使用大屏幕实时展示网络安全竞技过程。

竞赛环境依据竞赛需求和职业特点设计，在竞赛不被干扰的前提下安全开放部分赛场。观摩人员需佩戴观摩证件在工作人员带领下沿指定路线、在指定区域内到现场观赛。

十八、竞赛直播

本赛项赛前对赛题保密、设备安装调试、软件安装等关键环节进行实况摄录。竞赛过程采用实况转播的形式，对竞赛的开闭幕式、竞赛过程全程摄录。

本赛项在赛后将制作大赛制作优秀选手采访、优秀指导教师采访、裁判专家点评和企业人士采访视频资料。

十九、资源转化

赛后内向大赛办公室提交大赛成果资源转化方案如下表，半年内

完成资源转化工作。

资源名称			表现形式	资源数量	资源要求	完成时间
基本资源	风采展示	赛项宣传片	视频	1	15 分钟以上	赛后 30 天
		风采展示片	视频	1	10 分钟以上	赛后 30 天
	技能概要	技能介绍 技能要点 评价指标	文本资料	3	电子版资料	赛后 60 天
	教学资源	专业教材	文本资料	1	电子教材	赛后 180 天
		技能训练指导书	文本资料	1	电子教材	赛后 180 天
		大赛作品集	文本资料	1	电子版资料	赛后 180 天
		技能操作规程	文本资料	1	电子版资料	赛后 180 天
拓展资源	案例库		文本资料	1	电子版资料	赛后 60 天
	素材资源库		仿真课件	1	电子版资料	赛后 180 天
	赛题库		文本资料	1	电子版资料	赛后 60 天
	衍生成果		文本资料	1	电子版资料	赛后 180 天
	访谈视频		视频	1	10 分钟以上	赛后 60 天

赛后还需加强师资队伍建设，促进资源转化成果能够在教学中有效应用。

二十、其他

无

附件：样题

全国职业院校技能大赛（中职组）
网络安全竞赛试题
（总分 100 分）

赛题说明

一、竞赛项目简介

“网络安全”竞赛共分 A.基础设施设置与安全加固；B.网络安全事件响应、数字取证调查和应用安全；C.CTF 夺旗-攻击；D. CTF 夺旗-防御等四个模块。竞赛时间安排和分值权重见表 1。

表 1　竞赛时间安排与分值权重

模块编号	模块名称	竞赛时间（小时）	合计
A	基础设施设置与安全加固	3	20%
B	网络安全事件响应、数字取证调查和应用安全		40%
C	CTF 夺旗-攻击	3	20%
D	CTF 夺旗-防御		20%
总计		6	100%

二、竞赛注意事项

1.竞赛期间禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

2.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。

3.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。

4.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。

5.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。

6.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。

竞赛内容

模块 A 基础设施设置与安全加固

（本模块共 20 分）

一、项目和任务描述

假定你是某企业的网络安全工程师，对于企业的服务器系统，根据任务要求确保各服务正常运行，并通过综合运用登录和密码策略、数据库安全策略、流量完整性保护策略、事件监控策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力。本模块要求对具体任务的操作截图并加以相应的文字说明,并以 word 文档的形式书写,以 PDF 格式保存,并以赛位号作为文件名.

二、服务器环境说明

IDS:入侵检测系统服务器(Snort),操作系统为 Linux

LOG:日志服务器(Splunk),操作系统为 Linux

Web:IIS 服务器,操作系统为 Windows

Data:数据库服务器(Mysql),操作系统为 Linux

三、具体任务

任务一　登录安全加固

1. 密码策略（IDS,LOG,Web,Data）

   a. 最小密码长度不少于 12 个字符;

2. 登录策略（IDS,LOG,Web,Data）

   a.在用户登录系统时，应该有“For authorized users only”提示信息;

3. 用户权限分配(WEB)

   a.禁止来宾账户登录和访问;

任务二　数据库加固（Data）

1.以普通帐户安全运行 mysqld，禁止 mysql 以管理员帐号权限运行;

2.删除默认数据库(test);

任务三　Web 安全加固(Web)

1.删除默认站点;

2.限制目录执行权限,对图片或者上传目录设置执行权限为无；

任务四　流量完整性保护（Web,Data）

1.HTTP 重定向 HTTPS，仅使用 HTTPS 协议访问网站（Web）；

2.防止密码被窃取，仅使用证书登录 SSH（Data）。

任务五　事件监控

1. Web 服务器开启审核策略：

   登录事件 成功/失败;

   特权使用 成功;

   策略更改 成功/失败;

进程跟踪 成功/失败;

任务六 服务加固 ssh\vsftpd

1.修改 ssh 服务端口为 2222;

2.ssh 禁止 ROOT 用户远程登录;

任务七 防火墙策略

所有服务器开启防火墙,为防止勒索病毒攻击对防火墙进行加固策略:

1.Windows 系统禁用 445 端口;

2.Linux 系统禁用 23 端口;

模块 B 网络安全事件、数字取证调查和应用安全

(本模块共 40 分)

一、项目和任务描述:

假定你是某网络安全技术支持团队成员,某企业的服务器系统被黑客攻击,你的团队前来帮助企业进行调查并追踪本次网络攻击的源头,分析黑客的攻击方式,发现系统漏洞,提交网络安全事件响应报告,修复系统漏洞,删除黑客在系统中创建的后门,并帮助系统恢复正常运行。

二、服务器环境说明

操作系统:Windows/Linux

三、具体任务

任务一　数据分析

1.使用 Wireshark 查看并分析 xxx 桌面下的 capture.pcapng 数据包文件，找出 telnet 服务器的用户名和密码，并将密码作为 Flag 值提交。

2.使用 Wireshark 查看并分析 xxx 桌面下的 capture.pcapng 数据包文件，ftp 服务器已经传输文件结束，将登陆服务器后的第一条指令作为 Flag 值提交。

3.使用 Wireshark 查看并分析 xxx 桌面下的 capture.pcapng 数据包文件，web 服务器地址是 192.168.181.250， 其使用的脚本语言为 php，将服务器使用 php 的版本号作为 Flag 值提交。

4.使用 Wireshark 查看并分析 xxx 桌面下的 capture.pcapng 数据包文件，这些数据中有非常多的 ICMP 报文，其中有一个设备是路由器，IP 地址为 192.168.181.25，将路由器上主动发出的 ping 请求的数量作为 Flag 值提交。

任务二 数字取证

1.黑客成功进入了 windows2008 中并且创建了多个用户，将黑客创建的用户名作为 flag 值提交｛名字 1-名字 2-.....｝。

2.查找黑客登录 ip，将 ip 地址进行提交。

3.黑客对数据库进行了多次暴力破解，将破解次数作为 flag 值提交。

4.查找黑客成功破解数据库时间，将改时间作为 flag 值提交。

任务三 内存取证

1.从内存中获取到用户 admin 的密码并且破解密码，以

flag{admin,password}形式提交(密码为 6 位)；

2.获取当前系统 ip 地址和主机名，以 flag{主机名,ip}形式提交；

3.桌面上有一个 flag 文件，请获取 flag 文件中的内容；

4.恶意进程在系统中注册了服务，请将服务名以 flag{服务名}形式提交；

任务四 漏洞扫描与利用

1.通过本地 PC 中渗透测试平台 Kali2.0 对服务器场景 Windows2020 进行系统服务及版本扫描渗透测试，并将该操作显示结果中 3389 端口对应的服务版本信息字符串作为 Flag 值提交；

2.在 msfconsole 中用 search 命令搜索 MS12020 RDP 拒绝访问攻击模块，并将回显结果中的漏洞披露时间作为 Flag 值（如：2012-10-16）提交；

3.在 msfconsole 中利用 MS12020 RDP 拒绝访问漏洞辅助扫描模块，将调用此模块的命令作为 Flag 值提交；

4.在第 3 题的基础上查看需要设置的选项，并将回显中必须要设置的选项名作为 Flag 值提交；

5.使用 set 命令设置目标 IP（在第 4 题的基础上），并检测漏洞是否存在，运行此模块将回显结果中第一行第四个单词作为 Flag 值提交；

任务五 Windows 操作系统渗透测试

1.找到任务服务器网络适配器信息，将首选 DNS 服务器地址作为 Flag 值提交；

2.找到桌面上 111 文件夹中后缀为.docx 的文件，将文档内容作为 Flag 值提交；

3.找到桌面上 222 文件夹中的图片文件，将图片中的英文单词作为 Flag 值提交；

任务六　应急响应

1.黑客通过网络攻入本地服务器，在 Web 服务器的主页上外挂了一个木马链接，请你找到此链接并删除链接，将删除链接后的主页第一排标题栏显示的第三个单词，作为 flag 提交。

2. 黑客攻入本地服务器的数据库服务器，并添加了除 admin 以外的具有一个管理员权限的超级用户，请你找到此用户并删除用户，将此用户名及密码作为 flag 提交。

模块 C　CTF 夺旗-攻击

（本模块共 20 分）

一、项目和任务描述

假定你是某企业的网络安全渗透测试工程师，负责企业某些服务器的安全防护，为了更好的寻找企业网络中可能存在的各种问题和漏洞。你尝试利用各种攻击手段，攻击特定靶机，以便了解最新的攻击手段和技术，了解网络黑客的心态，从而改善您的防御策略。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录攻击机。

二、操作系统环境说明

客户机操作系统：Windows 10

攻击机操作系统：Kali Linux 2019 版

靶机服务器操作系统：Linux/Windows

三、漏洞情况说明

1.服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.靶机服务器上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限;

3.靶机服务器上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限;

4.靶机服务器上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权;

5.操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限;

6.操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限;

7.操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

四、注意事项

1.不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

2.Flag 值为每台靶机服务器的唯一性标识，每台靶机服务器仅有 1 个；

3.选手攻入靶机后不得对靶机进行关闭端口、修改密码、重启或者关闭靶机、删除或者修改 flag、建立不必要的文件等操作；

4.在登录自动评分系统后，提交靶机服务器的 Flag 值，同时需要

指定靶机服务器的 IP 地址；

5. 赛场根据难度不同设有不同基础分值的靶机，对于每个靶机服务器，前三个获得 Flag 值的参赛队在基础分上进行加分，本阶段每个队伍的总分均计入阶段得分，具体加分规则参照赛场评分标准；

6.本环节不予补时。

模块 D　CTF 夺旗-防御

（本模块共 20 分）

一、项目和任务描述

假定各位选手是某安全企业的网络安全工程师，负责若干服务器的渗透测试与安全防护，这些服务器可能存在着各种问题和漏洞。你需要尽快对这些服务器进行渗透测试与安全防护。每个参赛队拥有专属的堡垒机服务器，其他队不能访问。参赛选手通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能。

请根据《赛场参数表》提供的信息，在客户端使用谷歌浏览器登录需要加固的堡垒服务器。

二、操作系统环境说明

客户机操作系统：Windows 10

攻击机操作系统：Kali Linux 2019 版

堡垒服务器操作系统：Linux/Windows

三、漏洞情况说明

1.堡垒服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.堡垒服务器上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限;

3.堡垒服务器上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限;

4.堡垒服务器上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权;

5.操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限;

6.操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限;

7.操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

四、注意事项

1.每位选手需要对加固点和关键过程截图，并自行制作系统防御实施报告，最终评分以系统防御实施报告为准。

2.系统加固时需要保证堡垒服务器对外提供服务的可用性；

3.不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

4.本环节不予补时。