年　度	2022
编　号	QGB202201

2022年度“强国杯”技术技能大赛

——网络和数据安全应用技术赛项

技术方案

2022 年 06 月

目 录

一、大赛名称 1
二、大赛意义 1
三、大赛内容、形式和成绩计算 2
（一） 竞赛内容 2
（二） 竞赛形式 4
（三） 参赛对象 5
（四） 报名条件 5
（五） 成绩计算 5
（六） 晋级规则 6
四、奖励办法 7
五、命题范围、赛题类型和其他 7
（一） 命题原则 7
（二） 实操技能考核 8
六、大赛场地与设施 8
（一） 大赛场地 8
（二） 大赛设施 10
七、大赛议程与时间安排 11
（一） 关键环节 11
（二） 竞赛流程 11
（三） 时间安排 13
八、大赛赛题 13
九、大赛评分标准制定原则、评分方法、评分细则及技术规范 14

（一） 评分标准制定原则 14
（二） 评分方法 14
（三） 评分细则(评分指标) 14
（四） 评分方式 16
（五） 技术规范 16
十、大赛平台说明 16
十一、大赛安全保障 18
（一） 大赛保障 18
（二） 大赛应急预案 19
十二、大赛组织与管理 20
（一） 大赛设备与设施管理 21
（二） 大赛监督与仲裁管理 21
十三、裁判人员要求 22
十四、疫情防控 23

一、大赛名称

2022年度“强国杯”技术技能大赛——网络和数据安全应用技术赛项

二、大赛意义

为贯彻落实习近平总书记关于人才工作重要论述，落实中央人才工作会议精神，大力培育支撑制造强国、网络强国建设的技术技能人才队伍。工业和信息化部教育与考试中心决定举办2022年度“强国杯”技术技能大赛。

本次大赛以人才选拔和培养为宗旨，为全国工业和信息化领域培育和选拔一大批素质优良、结构合理的高素质技术技能人才队伍，服务“两个强国”建设。

2016年12月27日，我国发布《国家网络空间安全战略》，战略要求“保护网络空间信息依法有序自由流动，保护个人隐私，保护知识产权”；国家“十四五”规划更明确提出“加强网络安全保护”，并具体指出要“加强重要领域数据资源、重要网络和信息系统安全保障”，相关部署将持续推动数据安全行业发展。

当前，网络空间安全斗争普遍日趋尖锐复杂，关键信息基础设施、重要数据和个人隐私都面临新的威胁和风险。要打赢网络安全这场战争，培养符合要求的网络空间安全人才是解决网络安全问题的关键所在。安全人才的聚合，才能产生自生长的安全能力。

“强国杯”比赛提供了一个优秀的平台，参与者能够综合运用各种手段，进行漏洞挖掘和有效利用，开展数据取证分析和积极防御，像攻击者一样来思考问题，在攻防过程中完成自我成长。在竞赛过程中选手或主动或被动，补全计算机和网络安全基础理论知识、网络和数据安全的攻防能力，培养了从理论转向实践的能力，并且能够在安全领域结合

业务活学活用。展示参赛选手文明生产意识和团队合作精神，培养高素质技术技能人才，聚焦新职业，助力后疫情时代职业技术教育发展，凸显职业教育的重要性。

三、大赛内容、形式和成绩计算

（一） 竞赛内容

竞赛内容包括操作系统安全、数据库安全、网络层攻击与防护、Web应用安全、渗透测试技术、应急响应与恢复、软件开发安全、恶意代码与逆向、移动应用安全等，通过不同的赛制模式将知识点和赛题结合向选手呈现。

1.操作系统安全检测与防护

了解操作系统（Windows、Linux、Unix等）的常规安全防护机制。熟悉系统日志、应用程序日志等溯源攻击途径。掌握系统账号、权限、文件系统、文件共享、网络参数、端口、服务、日志审计和漏洞补丁等项目的安全检测与安全加固方法；掌握系统加密、系统防火墙、安全策略和杀毒软件的安装和配置方法。

2.数据库安全检测与防护

了解数据库（Mssql、Mysql、Oracle、MongoDB）的库表管理、数据访问、权限控制等基础安全防护机制。熟悉数据存储加密不当、数据库访问与权限管理配置不当、SQL注入攻击、数据库漏洞攻击等常见安全问题。掌握数据库运维管控、数据存储加密、数据脱敏、风险发现和日志审计等安全防护方法。

3.网络层攻击与防护

了解网络层的网络架构、传输方式、传输协议和控制措施；了解针对有线和无线的攻击方式和安全防护机制。熟悉常见的网络层攻击，包

括：DoS和DDoS、窃听、假冒/伪装、重放攻击、篡改、针对DNS的工具（欺骗、投毒和劫持）、ARP攻击、DHCP攻击以及无线攻击等。掌握通过使用网络层安全工具和设备（如：NMAP、防火墙、Web防火墙、IDS/IPS、抗拒绝服务攻击系统、网络扫描器等）发现和阻断网络层攻击的方法和技术；掌握对网络层设备（如：路由器、交换机等）的安全配置和加固技术；掌握验证各种安全防护手段（如密码强度、访问控制）有效性和强度的方法。

4.Web应用安全

了解Web应用安全架构，风险分析及常规防护思路。熟悉框架和组件漏洞、权限绕过、弱口令、注入、跨站、文件包含、非法上传、非法命令执行、任意文件读取和下载等常见安全问题。掌握常见Web环境的安全配置方法、检测方法和安全防护手段。

5.渗透测试技术

熟悉渗透基本思路、方法和流程，熟悉各种常见渗透测试工具。掌握常规的渗透测试技术，包括：信息收集、漏洞发掘、常规漏洞利用、常见应用入侵、服务器提权、远程溢出攻击、内网渗透、身份隐藏和暗网挖掘等。

6.应急响应与恢复

熟悉应急响应与恢复的基本方法和流程。掌握应急响应和恢复的调查、取证、恢复等相关技术，包括：入侵取证分析、日志审计分析、反取证技术、文件删除恢复和中毒文件恢复等。

7.软件开发安全

了解软件安全开发生命周期、软件安全架构和设计、软件威胁建模原理和方法；了解常见编程环境（C/C++、JAVA、PHP、JSP等）的构建以

及语言的编写。熟悉常见的软件安全漏洞的产生原理和加固方法；熟悉软件安全开发过程中有关参数化查询、输入验证、输出编码、访问控制、身份验证、安全日志、API接口安全、使用安全的第三方组件等安全开发规范；熟悉代码审计（包括人工审计和工具审计）和代码加固技术。

8.恶意代码与逆向

熟悉恶意代码的分类、特点和运行机制，熟悉常见的恶意代码，包括：后门、僵尸网络、启动器、感染病毒、远程控制木马、Rootkit等。熟悉发现、隔离、清除常见恶意代码的相关工具及技术手段。熟悉常见的恶意代码保护措施以及清除手段。熟悉对常见恶意代码进行静态与动态的分析、源定位以及修复的方法。

9.移动应用安全

了解智能终端操作系统（安卓系统、苹果IOS）的安全机制；了解移动应用软件的安全机制和调试分析、代码审计技术。熟悉移动互联网联网应用和应用商店的架构组成与技术实现；熟悉移动应用软件的越权访问、信息泄露、上传漏洞、业务逻辑错误等安全问题的检测与处理技术；熟悉针对移动应用程序的安全防护技术。掌握移动互联网恶意程序的监测与处置方法。

（二） 竞赛形式

线上选拔赛、线上分区赛采用团队网络安全解题模式（CTF），参赛队伍限制4人（1名教练+4名参数选手）。参赛队伍可以通过互联网参与，以解决网络安全技术挑战题目的分值和时间来排名。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

线下总决赛采用解题+攻防的混合模式，解题赛赛制和选拔赛相同。

团队攻防对抗赛（AWD），每支队伍4人，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御避免失分。可以实时通过得分反映出比赛情况，最终以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力同时也比团队之间的分工配合与合作。

（三） 参赛对象

参赛对象：全国高职院校、应用型本科院校在校学生

（四） 报名条件

线上初赛每支参赛队不可超过4人，每队可额外配一名教练，教练不可参赛，以赛队为单位进行初赛；参赛选手必须是中国合法公民，需要提交队伍名称、学校信息、联系电话等信息，报名截止后不得修改报名信息及增加报名人员；入围决赛的队伍成员必须是已经报名的成员，未报名的选手无法代表队伍参赛，参赛成员需要在规定时间内提供身份证、学生证材料用于线下比赛身份信息核实。

（五） 成绩计算

1.线上选拔赛和线上分区赛成绩计算规则

采用动态积分模式，每道题目初始分值为1000分，题目分数会随着解出人数的增加而动态减少，例如题目A当只有1个人解出时题目分值为1000分，2个人解出是题目分值为909分，题目分值到45分时便不在减少。每道题目前三名解出的选手有额外奖励分，奖励分计算方式为当前分值的5%、3%和1%，第4名及后续选手不获得奖励分。奖励分的分值会随着题目分值的减少而减少。当出现相同分值的情况根据时间进行排名，

即达到这一分值用时较少的队伍排名靠前。

解题赛动态积分公式以题目解出人数作为动态积分的变量，目前根据解题人数划分了4个阶段，分别对应不同的积分公式，对应关系如下（X代表解出人数）：

（1）当0=X时，公式f(x)=1000分

（2）当0<X≤30时，公式f(x)= 300+ [（51-x）/50]³ * 700

（3）当30<X≤200时，公式f(x)= 46+ [（201-x）/170]²* 300

（4）当200<X时，公式f(x)=45

2.线下总决赛成绩计算规则

（1）解题赛成绩计算规则

采用动态积分模式，每道题目初始分值为1000分，题目分数会随着解出人数的增加而动态减少，例如题目A当只有1个人解出时题目分值为1000分，2个人解出是题目分值为909分，题目分值到45分时便不在减少。每道题目前三名解出的选手有额外奖励分，奖励分计算方式为当前分值的5%、3%和1%，第4名及后续选手不获得奖励分。奖励分的分值会随着题目分值的减少而减少。当出现相同分值的情况根据时间进行排名，即达到这一分值用时较少的队伍排名靠前。动态积分公式和线上选拔赛公式相同。

（2）团队攻防对抗赛成绩计算（AWD）规则

采用零和机制，每支参赛队伍有相同的初始分值，挖掘网络服务漏洞并攻击对手服务取得flag获得积分，被攻击方扣减相应分数；修补自身服务漏洞进行防御来避免丢分，最终以得分高低进行排名。

（六）晋级规则

线上选拔赛成绩按照东、南、西、北四个区域划分，进行单独排

名，每个区域选拔前50名的队伍入围线上分区赛。自动放弃入围分区赛资格的名额依次顺延。入围战队赛后审核存在作弊行为的判定自动放弃入围分区赛，名额依次顺延。

线上分区赛每个区域单独办赛，选拔当前区域的前10名队伍入围线下总决赛。自动放弃入围分区赛资格的名额依次顺延。入围战队赛后审核存在作弊行为的判定自动放弃入围分区赛，名额依次顺延。

四、奖励办法

组委会颁发一、二、三等奖奖项，并颁发获奖证书，获奖比例：一等奖占报名队伍的10%；二等奖占报名队伍的20%；三等奖占报名队伍的30%；对一等奖获奖队伍的教练（每支参赛队伍指定1名教练），颁发“优秀教练”证书;对贡献突出的承办、协办和技术支持单位，颁发“突出贡献单位”奖牌和证书；对大赛组织实施中表现突出的个人，颁发“优秀工作者”证书；对在各赛项执裁工作中表现突出的个人，颁发“优秀裁判员”证书。

大赛设置总奖金池6.9万元。包含金银铜三个奖项，按照最终成绩的排名进行颁发。

奖项类别	奖项数量	奖金
金奖	第1名-第3名	每队1万元，共3万
银奖	第4名-第9名	每队3000元，共1.8万
铜奖	第10名-第30名	每队1000元，共2.1万

五、命题范围、赛题类型和其他

（一） 命题原则

按照信息安全专业人员（CISP）考试大纲为出发点，结合我国网络

基础设施和重要信息系统安全保障的实际需求，以知识体系的全面性和实用性为原则，突出职业技能能力考核及工匠精神要求。本次赛题通过梳理知识体系，定制符合参赛人员能力水平为原则，定向筛选出一大批素质优良、结构合理的高素质技术技能人才队伍为目标。

（二） 实操技能考核

考核范围：web、pwn、misc、crypto、reverse和mobile赛题方向。

考核题型：题型为附件题、场景题。

考核时间：只计算正常比赛的时间，不计算单个题目的解题时间，选手在规定时间都可以进行解题。

考核方式：参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给平台，从而夺得分数。。

命题方式：所有题目均来自360技术团队，通过对经典CVE的复现、二次修改或1day题目。

六、大赛场地与设施

（一） 大赛场地

大赛场地需要满足竞赛设备、参赛人员和观摩人员的入场。大赛场地按照承载的不同功能详细划分为签到区、检查区、选手区、运维区、观摩区区域。

1.签到区

设置在住宿酒店的的入口处，设置签到板和纸质文件，抵达酒店的参赛选手须在纸质文件进行签到并领取手提袋（包含赛事相关资料）。签到板可自行根据意愿选择签字。

在正式比赛当天，进入比赛场地前同样需要进行签到。

2. 检查区

竞赛场地签到完成后，进入检查区。如果竞赛期间不允许上网，工作人员会按照相关规定进行检查如上缴手机、确认笔记本电脑数量、核实人员信息（身份证、学生证）确认为本人参赛。若发现非本人参赛立即向赛事组委会反馈，并按照赛事章程进行处理，等赛组委会的处罚决定。

3. 选手区

完成检查区的人员信息后，根据座次表和桌面队旗指引，各参赛人员有序进场，检查桌面网络、电源是否满足使用需求，确认无误后签写网络确认单并交给现场工作人员。若发现桌面环境不满足参赛需求，请及时报告工作人员，解决后签写网络确认并交给现场工作人员。

4. 运维区

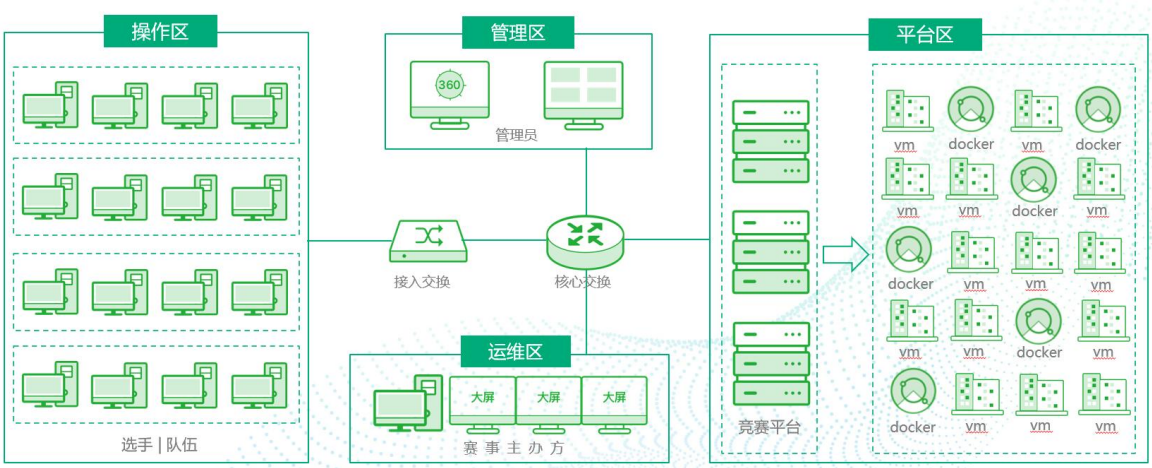
运维区是运维人员的工作场地，包括项目经理、平台运维、网络运维、题目运维。本区域禁止非竞赛运维相关人员进入，防止其他人在此区域获取赛事相关信息并泄露给参赛人员。

5. 观摩区

观摩区为教练和参观人员观摩比赛成绩的区域，通过大屏播放成绩排行榜和态势展示两种内容，并安排1名工作人员对态势内容进行讲解，让观摩人员能够理解态势展示元素，通过3D态势的元素变化来了解选手的解题进度。

6. 局域网部署

大赛场地部署单独局域网满足竞赛需求，选手通过局域网访问竞赛平台和赛题环境，观摩区通过网络访问大赛排行榜和3D态势。



7. 强弱电部署要求

强电部署需要遵循分区域部署，选手区、运维区、观摩区进行分闸配电，每个区域之间互不影响，一个电闸负责一个区域。

（二）大赛设施

明确大赛平台、耗材、工具仪器、防护装备、禁止携带物品等。

1. 线上选拔赛

名称	单位	数量	备注
360网络攻防竞赛平台	套	1	
高性能云主机	台	若干	满足竞赛需求
高抗DDOS	次	1	

2. 线上分区赛（每个区域1套）

名称	单位	数量	备注
360网络攻防竞赛平台	套	4	
高性能云主机	台	若干	满足竞赛需求
高抗DDOS	次	1	

3. 线下总决赛

名称	单位	数量	备注

360网络攻防竞赛平台-管理平台	台	2	1主1备
360网络攻防竞赛平台-计算平台	台	若干	满足竞赛需求
强三层核心交换机	台	1	
三层接入交换机	台	若干	满足竞赛需求
桌面交换机	个	若干	满足竞赛需求
3m桌面跳线	条	若干	满足竞赛需求

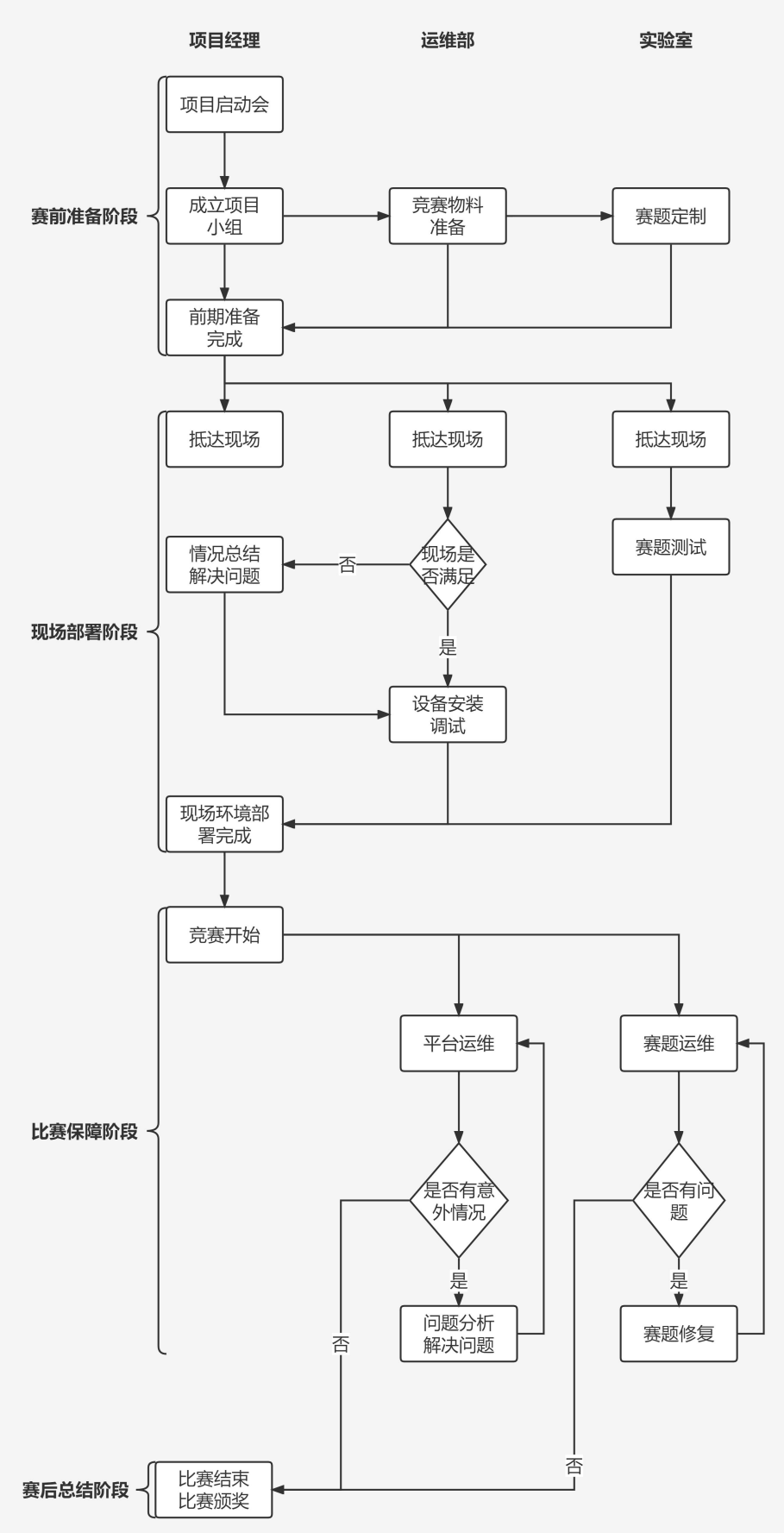
七、大赛议程与时间安排

（一） 关键环节

参赛选手报到——参赛选手赛前熟悉场地、领队会——开幕式——正式比赛 ——比赛结束（参赛选手上交比赛成果）——成绩评定——大赛技术点评、颁奖 仪式、闭幕式。

（二） 竞赛流程

竞赛管理基本流程可通过图来表达。竞赛管理基本流程


项目经理
运维部
实验室
项目启动会
赛前准备阶段
成立项目小组
竞赛物料准备
赛题定制
前期准备完成
抵达现场
抵达现场
抵达现场
现场部署阶段
情况总结解决问题
否
现场是否满足
赛题测试
是
设备安装调试
现场环境部署完成
竞赛开始
比赛保障阶段
平台运维
赛题运维
是否有意外情况
是否有问题
是
是
问题分析解决问题
赛题修复
否
否
赛后总结阶段
比赛结束比赛颁奖

（三） 时间安排

对接竞赛指南日程安排，根据全国疫情的情况，后续发布具体的时间安排。

（1）大赛组委会会议：2022年6月

（2）技术说明：2022年6月

（3）线上报名：2022年6月-7月8日

（4）线上选拔赛：2022年7月

（5）线上分区赛：2022年8-9月

（6）线下总决赛：2022年9月-12月

（7）颁奖仪式：大赛结束后颁奖。

八、大赛赛题

大赛组委在赛前15个工作日内组织技术说明会，并在大赛官方网站上发布比赛样题及大赛支撑平台的使用说明手册，初步定义提供的样题列表如下。（样题仅作为解题形式参考，正式赛题和样题存在差异化）

CTF解题赛		
题目方向	**题目类型**	**题目数量（道）**
WEB	场景	2
PWN	场景	1
CRYPTO	附件	2
REVERSR	附件	1
MISC	附件	1
MOBILE	附件	1
AWD团队攻防赛		
题目方向	**题目类型**	**数量（道）**

WEB	场景	1
PWN	场景	1

九、大赛评分标准制定原则、评分方法、评分细则及技术规范

（一） 评分标准制定原则

依据参赛选手完成的情况实施综合评定。评定依据2022年度“强国杯”技术技能大赛——网络和数据安全应用技术赛项竞赛实施方案中明确的技术规范，按照技能大赛技术裁判组制定的考核标准进行评分，全面评价参赛选手职业能力的要求，本着“科学严谨、公正公平、可操作性强、突出工匠精神”的原则制定评分标准。

（二） 评分方法

1.基本评定方法

裁判组在坚持“公平、公正、公开、科学、规范”的原则下，各负其责，按照制订的评分细则进行评分。现场评分：裁判组在比赛过程中对参赛选手的安全文明生产以及系统安装调试情况进行观察和评价进行现场评分。

成绩汇总：比赛成绩经过加密裁判组解密后进行加权计算，确定最终比赛成绩，经总裁判长审核、仲裁组长复核后签字确认。

2.相同成绩处理

线上选拔赛和分区赛当出现相同分数时以时间为依据，即先达到这一分数的排名靠前。

线下决赛当总分出现相同分数时以解题赛排名为依据，当解题赛分数也相同时根据攻防赛的排名为依据。

（三） 评分细则(评分指标)

1.线上选拔赛和分区赛评分细则

CTF解题赛:

选手通过解题获取题目内预置的flag，提交后平台会自动判断，正确flag增加相应得分，错误flag不得分，选手可多次提交flag，直至本道题目正确为止。

线上选拔赛采用动态积分模式，每道题目初始分值为1000分，题目分数会随着解出人数的增加而动态减少，每道题目前三名解出的选手会获得当前题目5%、3%和1%的额外奖励分值。最终排名以排行榜成绩为准。

2.线下总决赛评分细则

CTF解题赛:

选手通过解题获取题目内预置的flag，提交后平台会自动判断，正确flag增加相应得分，错误flag不得分，选手可多次提交flag，直至本道题目正确为止。

线上选拔赛采用动态积分模式，每道题目初始分值为1000分，题目分数会随着解出人数的增加而动态减少，每道题目前三名解出的选手会获得当前题目5%、3%和1%的额外奖励分值。

团队攻防对抗赛（AWD）:

团队攻防对抗赛采用零和机制，每支参赛队伍有相同的初始分，挖掘网络服务漏洞并攻击对手服务取得flag获得积分，被攻击方扣减相应分数；修补自身服务漏洞进行防御来避免丢分，最终以得分高低进行排名。

（1）比赛10分钟/回合，每个回合会更新GameBox上的flag。

（2）每个回合内，一个战队的一个服务被渗透攻击成功（被拿flag并提交），则扣除50分，攻击成功的战队平分这些分数。

（3）每个回合内，服务宕机或无法通过check则会被扣除50分，服务正常的战队平分这些分数。

（4）每个回合内，服务异常和被拿flag可以同时发生，即战队在一个回合内单个服务可能会被扣除两者叠加的分数。

最终成绩计算:

竞赛模式	赛制比重	最终得分计算公式
CTF解题赛	60%	（队伍得分/本场最高得分）*600
AWD对抗赛	40%	（队伍得分/本场最高得分）*400

当出现相同分数时以解题赛排名为依据，当解题赛分数也相同时根据攻防赛的排名为依据。

（四） 评分方式

竞赛过程中所有分数均由竞赛平台自动计算得出，不存在人工干预的情况。在出现违反竞赛规则的情况会进行取证、相关队伍对确认，组委会确认等环节进行扣分操作，扣分需要人工干预。

（五） 技术规范

严格按照组委会审核通过的竞赛规则为依据，平台自动化判分为最终结果，禁止人工干预大赛得分的行为（违反竞赛规则判罚不在此行为内）。

十、大赛平台说明

360网络攻防竞赛平台是360政企安全集团自研的新一代实战类网络安人才训练和竞技平台，为企业用户提供了多种安全竞赛模式、酷炫的3D态势、严格的防作弊技术、海量安全工具。平台采用国内领先的私有云技术，可以快速创建多场高度仿真的网络安全攻防训练和竞赛环境，是政府、金融、通信、能源、教育、部队等行业客户网络安全人才培

养、考核、选拔的首选产品。

产品架构：360网络攻防竞赛平台架构分为基础层、能力汇集层、应用层3个层面。

云平台层采用私有云虚拟化技术，支持KVM，Docker，SDN技术，将物理层资源进行虚拟化，提供存储、计算、网络能力的资源池，构建出符合复杂需求的场景拓扑，支持上层应用模块的资源调用。

能力汇聚层基于模块化的设计原则，提供资源中心、管控中心、数据中心三大模块。资源中心集中管理靶机、工具、赛题、试卷资源，为不同的竞赛演练提供高质量的可用资源。管控中心提供资源管控及系统运维类的功能，包含调度计算，镜像管理，安全管控，运维监控，日志模块。数据中心提供数据采集，数存储，数据处理，数据统计功能。能力汇聚层为版本的更新迭代提供强大的核心保障。

应用层部分提供面向普通用户、主办方和管理员的不同用户界面。包含4种竞赛模式，工具库及用户管理，仪表盘，3D态势，赛事管理，系统管理，运维管理的功能模块；应用层平台用户部分提供参赛选手及管

理人员的管理。选手包括账号、队伍，管理人员包括管理员及主办方。

十一、大赛安全保障

（一） 大赛保障

1.安全运维保障

负载均衡：竞赛平台采用集群+负载均衡方式进行部署，解决赛事期间容器的大并发压力，增强网络处理能力，减轻单个设备的资源压力，提供整体服务性能。

使用负载均衡方式，解决赛事过程中以下问题：

（1）解决并发压力，提供容器的处理性能（增加网络吞吐量，加强网络处理能力）。

（2）提供故障转移，实现高可用。

（3）通过添加或减少服务器数量，提供服务的伸缩性。

（4）增加防护过滤规则和白名单，增强安全防护性。

2.电力保障

服务器集群提供UPS储电设备，防止因市电停电的情况下导致数据丢失，影响赛事的正常进行。UPS提供的电力满足服务器满载状态下持续运行30分钟，在此期间完成数据备份、清空赛题环境资源和服务器正常关机，等待市电的重新供电。

3.运维区域隔离

现场人员划分，工作证区分，无相关证件者禁止入内。比赛场地的各个区域之间通过隔离带隔离，并安排工作人员监督出入口并对身份信息进行核对，防止无关人员进入。

4.人员安全保障

（1）进出口处须配置会务支持人员，设立体温检测岗，配洗手消毒

液，进入场馆的人员必须佩戴口罩，使用额温枪进行体温检测，一律凭证进入（一切与赛事无关人员等严禁进入，进入场馆后进行分区块管理，尽量避免人员交叉。

（2）场地须保证每天做好消毒工作。工作人员须每天对训练场馆内地面进行消毒，地面可用含有效氯浓度为500mg/L的含氟消毒剂喷洒。

（3）人员每天对竞赛场地内高频接触部位，可选用擦拭、喷雾的方法，一般选择有效氧浓度为500mg/L的含氯消毒剂，作用30分钟后再用清水擦拭干净，每天至少一次。

（4）场馆内应设立口罩回收专用垃圾箱，每天对回收垃圾袋内的口罩进行消毒，并清理转运。

5.生活条件保障

（1）赛事期间推荐的住宿地点均有宾馆或住宿的经营许可资质。

（2）用餐供应商均具有合格的营业执照和卫生许可证，为赛事期间提供午饭供应。根据国家民族相关的政策，按照少数民族的饮食习惯作为依据，完成赛事期间的饮食供应。

（3）大赛期间组织观摩活动的交通统一由赛事组委会负责，在赛事期间要保证好选手和教练的交通安全。

（二） 大赛应急预案

1.线上选拔赛

（1）快速恢复

在竞赛运维过程中，周期对系统数据进行备份存储，包括数据库数据，平台日志数据，配置数据等。当出现彻底中断事件时，如果备份服务器还存活，可以自动切换到备份服务器中的数据；如果服务器完全崩溃，通过重新部署服务器，安装虚拟化环境及系统的服务组件，导入运

维中备份的系统数据，进行数据灾难恢复。

（2）资源快速扩容

对于系统的临时扩容，运维人员针对加入集群的设备进行调试，完成集群一致性配置从而进行动态扩容。在将设备加入集群后后续过程由平台自动完成，且整个切换过程为无感切换。

2.线下总决赛

（1）性能保障

单台标准设备可满足不少于150个容器并发，根据队伍数量和题目资源使用需求，搭建满足比赛最大容器并发量且保证每个容器启动时间小于10s。

（2）快速扩容

使用自研的集群服务，计算节点服务器的选择可以同类型也可以不同类型，集群系统包含负载技均衡系统，会自动计算每台节点的可用资源进行智能下发任务，保证每台设备达到资源利用最大话。遇到节点资源小于并发资源时，集群系统支持自动化部署，预计10以内即可完成部署，加入集群局域网即可完成集群扩容。

（3）竞赛题目应急预案

每场比赛题目都预留了备用题目，防止题目出现故障或非预期解影响比赛公平的情况下，下线有问题的题目，使用备用题目替代，在保障比赛公平的前提继续进行。

竞赛过程中提供专业的支撑保障团队，一经发现题目的解题时间超出预期的情况的下，由网络运维人员下载相关解题流量，提供支赛题组进行分析，判断解题是否正常。

十二、大赛组织与管理

（一） 大赛设备与设施管理

大赛保障：360拥有专业的技术支持团队，旗下的网络安全实验室被誉为东半球最大的白帽子团队。近几年顺利支撑第十四届全国大学生信息安全竞赛创新实践能力赛-线上选拔赛和分区赛、第五空间网络安全大赛、津门杯网络安全创新竞技演示活动等国内大型网络安全竞赛。

赛场部署：赛场根据承载的不同功能进行区域划分，主要包括选手区、运维区和观摩区。每个区域通过隔离带隔离，现场分发工作证和参赛证，根据不同的证件前往不同的区域，严格执行区域隔离政策，保证赛事的顺利进行。区域间的强电要做好分路供电，防止出现连带情况。整个赛场通过局域网进行数据连接，完成承载不同功能的需求。

（二） 大赛监督与仲裁管理

大赛设置裁判组，负责赛制设计、题目设计、技术标准规及方案的制定，保证大赛技术的科学性、先进性、公平性和公正性。

1.防作弊机制

线上选拔赛和线下总决赛均提供严格的防作弊机制。线上选拔赛提供随机附件和独享动态flag防作弊机制，当发生作弊行为时，平台会自动判定作弊人员禁赛，管理员可以在后台查看到作弊信息。线下赛总决赛使用网络隔离和动态flag作弊。汇总作弊信息汇报组委会，由组委会判定最终结果。

2.场景题目-动态flag

竞赛平台的所有用户具有唯一的标示符：Token值，在创建赛题环境时，会依据选手的Token值进行动态flag的生成，保证全场唯一。当选手A把flag给选手B，选手B提交时，平台防作弊机制立即判定选手A和选手B作弊，禁止继续答题。后台可以查看作弊原因和解除禁赛状态，解除后

可正常答题。（作弊题目：题目1，作弊原因：选手B提交了选手A题目1的flag）

3.附件题目-随机附件

题目附件按照1:10准备（1个题目有10个flag，解题过程一样，只替换了最终解出的flag值），选手在下载附件时，系统随机匹配附件下载并记录，当选手提交的flag和系统记录不匹配时，系统会自动判定防作弊。

申诉流程&仲裁结果：在比赛过程中若出现有失公正或有关人员违规等现象，参赛队教练或队长可在比赛结束后30分钟之内向仲裁组提出书面申诉。赛项设仲裁委员会。大赛执委会办公室选派人员参加赛区仲裁委员会工作。赛项仲裁工作组在接到申诉后的10分钟内组织复议，并及时反馈复议结果。仲裁委员会的仲裁结果为最终结果。

十三、裁判人员要求

由重要行业部门相关领导、网络安全业内专家和大赛命题组部分成员组成。

1.工作原则

裁判长由李正吉担当。赛前建立裁判组。裁判组为裁判长负责制，负责比赛过程全程监督，防止营私舞弊。

赛事裁判组裁判长和裁判员。裁判员负责竞赛评分，由裁判长负责评分全过程，保证竞赛的公正与公平。

2.裁判评分方法

根据比赛环境，裁判组负责和选手沟通，技术支持工程师负责所有、设备应急。裁判员负责设备问题确认和执裁，技术支持负责执行裁判确认后的设备应急处理。

3. 成绩产生办法

竞赛评分严格按照公平、公正、公开的原则。

竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为，由裁判组按照规定扣减相应分数，情节严重的取消竞赛资格。选手有下列情形，需从比赛成绩中扣分:

（1）违反比赛规定，提前进行攻击或比赛终止后仍继续操作的，由裁判负责记录并酌情扣总分5%分。

（2）在竞赛过程中，违反操作规程，影响其他选手比赛的，未造成设备损坏的参赛队，扣总分10%分。

（3）在竞赛过程中，造成设备损坏或影响他人比赛、情节严重的报竞赛执委会批准，终止该参赛队的比赛，竞赛成绩以0分计算。

十四、疫情防控

（1）请各单位高度重视疫情防控要求，按照属地要求，提前做好相关准备工作，确保大赛 安全顺利进行。

（2）请各参赛队及各有关单位自大赛前第 14 天起，对所有参加大赛人员进行体温检测和健康状况监测。按照“异常人员应检尽检、其他人员愿检尽检”的原则，对身体状况出现异常和监测发现身体状况异常的人员进行核酸检测。

（3）请各参赛队及所有参加大赛人员出发前自行查验“一卡一码一证明”，即行程卡、健康码和核酸检测证明。低风险地区所有参加大赛人员需持健康通行码“绿码”，在测温正常且做好个人防护前提下可有序流动，进入密闭会场时需佩戴普通医用 口罩。中、高风险地区所有参加大赛人员需持有抵达前 7 日内核酸检测阴性证明和健康通行码“绿码”，在测温正常且做好个人防护前提下可有序流动，进入密闭会场时

需佩戴普通医用口罩。

（4）所有参加大赛人员体温低于37.3℃方可入场。身体状况异常的，大赛承办单位将协调卫生健康部门组织疾控机构和医疗机构专家对其进行核酸检测，并提出专业评估建议。

（5）疫情防控其他未尽事宜按属地疫情防控政策执行。