

附件2

大赛技术工作文件

2025年9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、竞赛安排	3
(一) 竞赛模块简介	3
1.职工组团队赛	3
(二) 命题说明（以职工组团队赛为例）	4
(三) 比赛时间、地点安排	4
(四) 评判标准（以职工组团队赛为例）	5
1.分数权重	5
2.评分规则	5
(五) 竞赛工作组	5
三、竞赛要求	7
(一) 注意事项	7
(三) 开放赛场要求	10
(四) 绿色环保要求	10
四、取消或推迟竞赛情况	11
五、竞赛题目大纲（以职工组团队赛为例）	11
六、竞赛进行方式	12
(一) 平台登录信息	12
(二) 登录平台	12
(三) 学员参加 CTF 竞赛	13
【操作步骤】	13
(四) 学员参加理论赛	16
七、竞赛标准及规范	18

一、技术描述

（一）项目概要

大赛赛事为网络安全知识竞赛与 CTF 夺旗赛，分为职工组与学生团体赛。竞赛形式包括网络安全知识竞赛与 CTF 夺旗赛。网络安全知识竞赛包括网络安全的法律法规、政策文件、通信网络安全防护标准、技术基础知识、日常应用等网络安全知识等，题型包括单选题、多选题、判断题。CTF 夺旗赛包括 web、溢出、逆向、隐写+综合、密码学、工业应用安全、工业协议安全、工控固件安全、车联网、5G 新技术新领域安全等类型。

（二）基本知识与能力要求

本项目选手应具备的知识点及特定技能参照世界技能大赛和中华人民共和国第一届职业技能大赛标准规范编制，可作为竞赛选手培养的指引，具体要求如下：

1.参赛选手需要掌握与网络安全事件响应、应用程序安全有关的国家职业标准及公认的行业和企业标准。

2.参赛选手需要了解夺旗赛（CTF）、实战相关攻防的技术、技能和要求。

3.主要考核技能：

（1）Web 安全相关的漏洞挖掘、漏洞利用、源代码分析等；

（2）运用各种数据算法对数据的加解密；

（3）计算机编程，包括计算机语言、编程、测试、调试；

(4) 分析计算机应用程序、软件或专用程序的安全性;

(5) 针对物联网、工控系统的安全分析;

4.对参赛选手考核的主要要求:按技术文件及测试项目规定进行规范操作。

5.职工组参赛对象:包括但不限于区内基础电信企业、宁夏铁塔公司、宁夏广电公司、互联网、工业、工业互联网、区内大中专院校教职工等相关从业人员。(参赛选手须为本单位员工,企事业单位的技术支撑机构不得以外援身份参赛)

6.学生组参赛对象:区内高等院校、高等职业院校(含技工院校)相关专业在校全日制在籍中职生、大专生、本科生、硕士生、博士生。学生组允许跨学校、跨学院组队,指导教师不得以选手身份参赛。

以下能力描述分为不同部分,每部分使用总分的百分比来表示它的重要性。竞赛测试项目及评分方案应尽可能的反映选手应具备的能力中所列知识点、技能,选手理论知识、工作能力的要求以及各项要求的权重比例如下表:

相关要求		权重比例 (%)
1	夺旗赛 (CTF)	
基本知识	—计算机网络基础知识 —密码学的基础知识 —常见的安全漏洞原理 —网络攻击原理与常见网络攻击方式 —常见恶意代码的类型和特征 —渗透测试的基础知识 —常用安全防护基础知识	30

工作能力	一了解并掌握网络体系结构的概念、主要的网络协议工作原理、组网的方法和技巧、路由和交换技术的原理以及网络故障检测和排除的基础知识等。 一了解并掌握密码学的基本原理，密码算法的分类以及常见加密、解密方式的实现原理等。 一了解并掌握缓冲区溢出、远程命令执行、注入、跨站等安全漏洞的原理、攻击方式和防御方法。 一了解并掌握钓鱼攻击的原理和步骤。 一了解并掌握病毒、蠕虫、特洛伊木马的原理和攻击方式等。 一了解并掌握信息收集、漏洞扫描、漏洞利用、提权、内网渗透等相关理论知识。 一了解并掌握身份鉴别、访问控制、安全审计、备份恢复等技术原理。	70
------	---	----

二、竞赛安排

（一）竞赛模块简介

1.职工组团队赛

模块编号	模块名称	工作任务	分数			备注
			理论分	实践分	合计	
A	网络安全知识竞赛	网安全理论知识答题，包括网络安全法律法规、政策文件、通信网络安全防护标准等，题型包括单选题、多选题、判断题。	100 分/人	0	300	比赛理论赛题与CTF同时开放，总时长3小时。其中，理论赛题只开放0.5个小时，比赛正式开始0.5小时后，理论赛题关闭。
B	CTF 夺旗赛	技能分析题，包含 web、溢出、逆向、隐写+综合、密码学等。	0	3200	3200	

2.学生组团队赛

模块编号	模块名称	工作任务	分数			备注
			理论分	实践分	合计	
A	网络安全知识竞赛	网安全理论知识答题，包括网络安全法律法规、政策文件、通信网络安全防护标准等，题	100 分/人	0	300	比赛理论赛题与CTF同时开放，总时长3小时。其中，理论赛题

		型包括单选题、多选题、判断题。				只开放 0.5 个小时，比赛正式开始 0.5 小时后，理论赛题关闭。
B	CTF 夺旗赛	技能分析题，包含 web、溢出、逆向、隐写+综合、密码学等。	0	3200	3200	

（二）命题说明（以职工组团体赛为例）

模块 A/B 共出 5 份试题，每一份试题都包含 40 道理论知识题，20 道 CTF 实操题目；

模块 A、B 总分为 3500 分，其中模块 A：每选手 100 分，总分 300 分；模块 B：3200 分。

（三）比赛时间、地点安排

1. 比赛时间及地点

职工组团体赛：

地点：

学生组团体赛：

地点：

2. 具体时间安排

时间	工作内容
X 月 XX 日 上午（职工 团体赛）	08:15~08:50 选手在学院南大门口签到领取选手证后，进入赛场，熟悉竞赛现场，进行设备试操作，赛事工作组复核选手身份信息、封存个人通信设备等。 08:50~08:59 宣布赛场须知，检查手机封存情况。 9:00~12:00 竞赛正式开始，各参赛小组进行知识竞赛及 CTF 夺旗赛答题。 12:00~12:30 裁判长、裁判组审核各小组答题得分情况并公布总成绩排名前 6 名的队伍。
X 月 XX 日 上午（学生 组团体赛）	08:30~09:00 选手签到，熟悉竞赛现场，进行设备试操作，赛事工作组封存个人通信设备等。 09:00~11:00 竞赛正式开始，各参赛小组进行知识竞赛及 CTF 夺

	旗赛答题。 11:00~11:30 裁判长、裁判组审核各小组答题得分情况，现场公布总成绩排名前 6 名的队伍。
--	---

（四）评判标准（以职工组团队赛为例）

1.分数权重

本次竞赛满分 3500 分。所有题目均为客观分值题，正确完成题目后即可获得对应分数。

2.评分规则

团队成绩=CTF 分数（3200 分）+个人理论赛分数（100 分）*3

说明：每一个 CTF 题目前三个解题的队员将得到额外奖励加分，比例为赛题分数的 10%，5%，3%。

提示：CTF 部分参赛选手可以根据自己特长自由选择答题顺序。

3.评判方法

竞赛系统根据各参赛选手提交的答题结果自动判卷并计算参赛选手成绩，按照成绩高低依次排名。

4.成绩并列

排名时，若成绩相同，根据最后提交正确答案的时间先后排名。

（五）竞赛工作组

1.竞赛裁判组

主要负责各赛项的现场评分裁决。

总裁判组：

总裁判长

副裁判长

裁判组：

组 长：

裁判员：

裁判职责：严格按照执裁流程和裁判岗位内容完成执裁工作，客观公正参加整个大赛制裁过程，严格监督并及时协调做好相关问题处理，对竞赛成绩进行认真汇总、审核、签字确认。

监审（仲裁）原则：总裁判组对总成绩复核，确认所有裁判员最终签字确认比赛成绩。如有人对比赛过程及比赛成绩提出异议、出现争议时，总裁判组负责收集和评估争议各方提交的证据，解决并处理竞赛过程中出现的技术性争议与纠纷、解决冲突，帮助当事双方达成和解或做出公正的决定。

2. 竞赛纪检组

督促技术组、裁判组等各工作组抓好赛风赛纪工作，监督检查竞赛各部门及相关人员廉洁自律、公平公正开展相关工作的情况。受理相关人员对赛事工作人员违纪违法问题和违规行为的检举、控告，研究、提出对赛事工作人员违纪违法违规行为的调查处理意见和建议。

组长：

组员：

3. 竞赛技术保障组

竞赛设施保障组对各赛项现场工位进行布置搭建、比赛设施设备调测、各赛项工具耗材准备、赛后耗材的处理等相关技术保

障工作。重点做好竞赛前期准备及保障选拔赛期间的工作任务。

组长：

成员：

4.竞赛赛务组

负责竞赛赛事准备、后勤服务、宣传制作等工作。重点做好赛前准备，裁判及参赛人员等相关赛事人员组织协调，保障竞赛期间的各项服务，现场摄影摄像及赛事宣传报道等工作。

组长：

成员：

5.竞赛安全保障组

负责竞赛期间健康和安​​全事务。主要包括检查竞赛场地、车辆交通及其周围环境的安全防卫；制定紧急情况应对方案；协调组织专业医疗、急救人员，做好安全突发事件等处理工作。

成员：

三、竞赛要求

（一）注意事项

1.本次比赛组委会不提供用于竞赛的计算机及相关外设，参赛选手须自带笔记本电脑（仅限一台，携带国标电源）进行答题。

2.场地禁止自带使用平板、手机、电子手表、多媒体播放器、录音器、照相机、摄影机等电子设备设备和材料；不允许携带包括 U 盘、移动硬盘在内的其他任何形式的存储介质。

3.比赛过程中所使用的各类技术工具均由参赛选手自行准备，大赛组委会不予提供。

4.每位选手机位上提供 RJ45 网线 1 条，参赛选手须根据自己笔记本电脑端口情况，自行携带 USB 转(或雷电、Type-C)转 RJ45 转接器等相关外设，确保所带外设能将笔记本电脑接入到比赛有线网络中。

5.选手的笔记本电脑推荐安装 Chrome 或 Firefox 浏览器。

6.平台默认启用多种反作弊机制，如果触发平台的反作弊机制，答题界面会直接显示异常信息，且主办方有权取消该队伍的比赛成绩。

(二) 选手要求

1.所有参赛选手须实名参赛，报到、入场及参赛时均须携带报名时使用的身份证原件，并接受现场工作人员检查。虚报信息、冒名顶替者一经查实，将被取消参赛资格。

2.参赛选手应严格遵守赛场规章、操作规范，保证人身及设备安全，接受裁判员的监督和警示，文明竞赛，遵守赛场秩序，禁止大声喧哗。不遵守赛场纪律，不听从赛场工作人员管理的取消参赛资格。

3.参赛选手按规定时间进入竞赛场地（竞赛开始后迟到 15 分钟及以上者不得进入赛场），按统一指令开始竞赛。在收到开赛信号前不得启动操作。各参赛人员自行决定答题顺序，在指定位置上完成竞赛项目。

4.比赛过程中可以组内交流；严禁跨组交流，禁止参赛队伍之间分享任何解题思路，发现违规者一律取消参赛资格。

5.竞赛选手不得查看竞赛答题系统以外任何网页，不得使

用任何社交软件（包括微信、钉钉、QQ、电子邮箱及其它任何带有社交功能的软件、通信平台），一经发现取消竞赛资格。

6.比赛过程中开放比赛现场的有线局域网,参赛选手均需通过 RJ45 网线接入竞赛网络,在竞赛系统进行作答,竞赛场地不提供互联网服务,也不允许选手以任何方式接入互联网。例如: 参赛选手不得在竞赛过程中开启使用个人手机热点,链接网络下载网络资源文件,赛场私自打开手机,私自开启使用手机热点的取消参赛资格。

7.选手应连续完成比赛,不得提前离开赛场。如需去卫生间请举手示意,经监考同意后方可前往。如特殊原因(如身体不适等)无法继续参赛的,需举手请示裁判,经裁判同意后方可离开赛场。选手离开赛场后不得在场外逗留,也不得再返回赛场。

8.竞赛现场如出现网络问题请举手,经裁判同意后可更换竞赛位置,更换过程中损失的时间计算在竞赛总时间内。除网络问题之外一切竞赛系统、题目问题均在竞赛系统内(通知栏问题答疑模块)咨询技术支撑组。

9.参赛选手须严格遵守赛场规章制度,服从裁判,文明竞赛。有作弊行为的,参赛选手所在队伍该项成绩为 0 分。如有不服从裁判、扰乱赛场秩序等行为,取消比赛资格和成绩。

10.竞赛期间,参赛选手严禁向竞赛系统、其他参赛选手个人电脑等发起任何可能影响比赛正常进度的攻击行为。嗅

探、攻击竞赛平台，故意影响他人竞赛，导致他人无法正常答题的取消参赛资格。

11.本次竞赛题目均不涉及需要借助对目标靶机的暴力破解、扫描等行为获取答案，为保障竞赛过程的稳定进行，不允许参赛选手对竞赛平台及目标靶机进行暴力破解和扫描。

12.在竞赛过程中，参赛选手须爱护赛场内的设施设备，注意用电安全。如因操作失误引起的设备损坏，由参赛选手承担相关责任。

（三）开放赛场要求

1.赛场内除指定的裁判、工作人员外，其他与会人员须经组委会同意或在组委会负责人陪同下，佩带相应的标志方可进入赛场内。

2.允许进入赛场的人员，只可在安全区内观摩竞赛，不得使用录像设备长时间拍摄选手工位、屏幕；不得与选手交谈，不得妨碍、干扰选手竞赛；不得在场内吸烟、喧哗。

3.经组委会允许的赞助商和负责宣传的媒体记者，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、干扰选手竞赛，不得有任何影响竞赛公平、公正的行为。

（四）绿色环保要求

1.环境保护：赛场严格遵守我国环境保护法，所有废弃物应有效分类并处理，尽可能地回收利用。

2.可持续性：工位将被用于为3个与技能相对应的模块进行测试。为了减少网络设备的数量，工位设备可用于多个模块的测试环境，比赛结束后设备可持续使用。

四、取消或推迟竞赛情况

1.如发生重大事故、疫情或上级领导部门发布限制通知、公告，可暂停或取消竞赛。

2.因各种原因现场发生群体性事件，导致竞赛无法进行，可取消竞赛。

3.竞赛平台因不可抗力导致无法正常进行竞赛，如停电、服务器大面积事故等，经裁判长决意后，可取消竞赛或推迟本次竞赛。

4.竞赛延长原则，竞赛环境出现故障小于 30 分钟则不延长竞赛时间，超过 30 分钟不足 1 小时得延长 30 分钟。超过 1 小时不足 2 小时的，延长 1 小时。

五、竞赛题目大纲（以职工组团队赛为例）

1.理论题 40 道。题目涉及网络安全的法律法规、政策文件、通信网络安全防护标准、技术基础知识、日常应用等网络安全知识。

2.CTF 题 40 道。按照初中高级题目进行出题，包含 web、溢出、逆向、隐写+综合、密码学。

3.详细赛题大纲

题目名称	题目分数	题目说明
理论题	300	单选+多选+判断
WEB	210	中级+高级
逆向	880	初级+中级+高级
溢出	160	中级

隐写+综合	980	初级+中级+高级
密码学	890	初级+中级+高级
工业互联网	80	中级

六、竞赛进行方式

（一）平台登录信息

参赛地址（建议谷歌浏览器）：

<http://192.168.11.252:30000/#/>

选手账号：报名手机号

默认密码：sitpassword@2024

首次登录平台需要重置密码，平台密码重置规则：

- 1.密码设计至少 10 位，最大 32 位
- 2.包括数字、小写字母、大写字母、特殊字母至少三种
- 3.口令应避免键盘排序

（二）登录平台

1.浏览器地址输入 <http://192.168.11.252:30000/#/>，进入登录页面，输入账号、密码及验证码，点击【登录】。

2.登录后进入首页，选择竞赛入口，进入竞赛平台。



(三) 学员参加 CTF 竞赛

【操作步骤】

1.进入竞赛平台后，查看到需要参加的赛事，点击【查看】进入赛事详情页。



2.赛事详情页可查看赛事简介、参赛资格、规则、奖惩措施，这些信息请在参加比赛前仔细阅读。



3.选择【赛项列表】，可查看积分的奖励规则。



4.到达比赛时间后，可点击【进入比赛】进入该场赛事主界面，这里展示该场比赛的试题，试题根据赛事情况逐步放出。在比赛进行中，遇到任何问题可通过页面小手呼叫裁判。



5. 点击【赛事题目】，查看该题详情。在该页面可以下载该题的附件、开启试题环境、销毁试题环境、提交 flag 等。Flag 支持多次提交。





6.根据大赛要求提交 writeup，请上传 pdf 格式的文件，如果上传多次，仅会保留最后上传的一份文档。



(四) 学员参加理论赛

1. 点击导航菜单【理论赛事】，进入理论赛页面；



2. 点击【进入考试】，进入试题详情页，按照提示进行答题，答题完成后提交试卷。提交试卷后不可再参加考试；



3. 考试完成后可查看理论赛成绩。成绩会随着提交人员名次会有更新。

我的考试		我的成绩		可查看试卷总分及成绩			请输入您要查询的信息	Q
考试名称	考试时间	考试用时	总题数	考试分数	考试人数	名次		
理论考	2022-06-15 11:57:46至2022-06-17 00:00:00	00小时00分00秒	4	0/8	1	1		
考试	2022-06-14 18:21:29至2022-06-15 00:00:00	00小时00分38秒	4	4/8	2	2		
理论卷测试	2022-06-13 16:44:31至2022-06-14 00:00:00	00小时02分00秒	4	0/8	2	1		
		共 3 条		10条/页	< 1 >	前往 1 页		

七、竞赛标准及规范

网络与信息安全管理员职业技能标准

信息系统安全保障评估框架 GB/T 20274.1-2006

信息系统安全保障评估框架 GB/T 20274.1-2006

信息安全管理实施细则 ISO/IEC17799 BS7799-1:2005)信息

安全管理体系-要求 ISO27001(BS7799-2:2005)

中华人民共和国计算机信息系统安全保护条例

商用密码管理条例

其他国家法律、法规、规章及规定