

# 2024 年柳州市职工职业技能大赛

## 网络与信息安全管理项目 技术工作文件

2024 柳州市职工职业技能组委会技术工作组

2024 年 6 月

# 目 录

一、赛项概述与技术标准 .....	3
二、竞赛形式 .....	4
三、试题和评判标准 .....	4
（一）理论知识竞赛要求 .....	4
（二）实操技能竞赛要求 .....	4
（三）比赛时间安排 .....	5
（四）评判标准 .....	6
四、竞赛规则 .....	6
（一）裁判员工作内容 .....	6
（二）选手的工作内容 .....	8
（三）问题或争议的处理 .....	9
五、大赛技术平台 .....	9
（一）场地基本设备工具清单表 .....	9
（二）基本材料清单表 .....	10
六、安全、健康要求 .....	11
（一）健康安全和绿色环保 .....	11
（二）项目特别规定 .....	12
七、竞赛流程和日程安排 .....	14
（一）竞赛流程 .....	14
（二）竞赛日程安排（以正式发布的比赛指南为准） .....	14
八、本竞赛项目的最终解释权归大赛组委会。 .....	15

## 一、赛项概述与技术标准

网络与信息安全管理员赛项的参赛对象为柳州市从事网络与信息系统安全工作的职工。按照《中华人民共和国职业分类大典（2022年版）》新增“数字职业”中“网络与信息安全管理员”所定义的职业内涵和工作任务作为本次大赛命题依据，要求参赛选手在比赛规定时间内完成信息安全领域的相关比赛任务。通过本项目竞赛，使选手能熟练运用网络信息安全技术进行信息系统的安全分析、安全架构、安全运维与监控等过程，为国家网络信息安全行业培养高素质的技术技能型人才。

鉴于参赛选手日常工作的主要职责是保障信息系统安全稳定运行，大赛将从政策法规标准和网络安全风险评估、安全防护、安全应急响应技术等方面，围绕信息系统的事前检测与防护、事中应急与防御、事后取证与溯源等技术要点展开，全方位考核从业职工的网络安全综合能力。

本工种比赛涉及的信息安全工程在设计、组建过程中，主要有以下 8 项国家标准，参赛选手在实施竞赛过程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》

## 二、竞赛形式

本工种比赛形式为个人赛，赛事共计二阶段，采用线下集中模式进行，比赛总用时为 5.5 个小时，比赛总成绩满分为 100 分。

第一场比赛安排在上午，设置理论知识竞赛，考试时间为 1 小时，理论知识竞赛成绩满分为 100 分，占总成绩的 30%。

第二场比赛安排在下午，设置实际操作技能比赛，比赛时间为 4.5 小时，实操技能比赛成绩满分为 600 分，占总成绩的 70%。

## 三、试题和评判标准

### （一）理论知识竞赛要求

理论知识竞赛为标准化考试，考试时间 60 分钟，题目内容包含但不仅限于风险评估、应急响应、渗透测试、网络安全法律法规等。题型有单项选择题、多项选择题、判断题，以现场线上答题的方式完成标准化的比赛评分。重点考核参赛选手网络安全常识、意识以及理论知识，具体包括：

1. 网络安全相关基础知识、法律法规、风险评估等；
2. 杂项包括图片隐写、压缩包隐写、音频隐写等理论知识；
3. 密码包括古典密码与现代密码，例：猪圈密码、RSA 等理论知识；
4. 逆向包括二进制逆向与 android 逆向，脱壳、反编译等理论知识；
5. WEB 包括常见漏洞题目，例：SQL 注入、文件上传、文件包含、CSRF、反序列化等理论知识。

### （二）实操技能竞赛要求

实操技能比赛将模拟真实应用系统在实际应用中为保障其安全稳定运行所涉及的工作，主要包括应急响应处置、操作系统安全、数

数据库安全、Web 应用、数据包分析、密码学、数据恢复、逆向分析、新技术新应用等。

1. 竞赛单元 1——CTF 夺旗赛（信息系统安全攻防及运维安全监控）

本单元为每位选手提供一台客户机和虚拟服务器，或单独一台虚拟服务器，选手对该服务器进行风险评估。该服务器存在不同等级的安全漏洞，参赛选手可通过手工方式或检测工具进行漏洞发现、渗透测试等风险评估工作，以及网络安全事件响应、数字取证调查等，该环节以提交指定答案的方式来完成比赛任务。在完成比赛任务过程中，提交的答案可能是一个数值或截图的方式，该模式采用 CTF 方式，分 4-5 个任务，每个任务 5-9 个题目，该环节以提交指定的答案（FLAG）或者将答案进行截图的方式进行提交。

2. 竞赛单元 2——AWD 攻防赛（含职业素养）

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，参赛选手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）比赛时间安排**

本项目比赛总时间为 5.5 个小时，分为 2 个阶段 1 天完成。

各模块时间分配如下表：

序号	模块名称	竞赛时间	权值
第一阶段	理论答题	1 小时	30%

第二阶段	CTF 夺旗赛	3 小时	35%
	AWD 攻防赛	1.5 小时	35%
总计		5.5 小时	100%

#### （四）评判标准

##### 1. 分数权重

序号	模块名称	权值	评分方式
第一阶段	理论答题	30%	客观评分
第二阶段	CTF夺旗赛	35%	机考评分
	AWD攻防赛	35%	机考评分
总计		100%	

##### 2. 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。

### 四、竞赛规则

#### （一）裁判员工作内容

裁判组下设若干裁判小组，每个裁判只能参加一个小组的执裁工作，各小组独立负责各自任务部分的竞赛过程的完整工作，相互之间不相重合。本项目的裁判必须严格按照执裁流程和裁判岗位内容完成

执裁工作，包括相关竞赛技术性文件学习。在执裁过程中需要全程参加整个执裁和评分过程，包括赛前的准备工作，场地、设备准备与检验，竞赛试题的调整与试做，评分标准的制定与确认，选手进场的抽签，执裁过程中的监督与问题处理，评分，竞赛成绩的汇总、审核、确认等。

1. 裁判长负责裁判组的技术工作，裁判的具体工作由裁判长在裁判培训会议上布置，裁判在执裁中必须服从裁判长和组委会的管理，遵守裁判的职业道德，文明裁判。

2. 裁判长根据工作需要和培训情况，对裁判员进行工作分工。

3. 裁判员应坚守岗位，不迟到早退。无特殊情况不得在竞赛期间请假。在执裁过程中需要暂时离开的，必须向裁判长申请，得到许可后方可离开。

4. 裁判员在执裁过程中不得故意妨碍、影响任何选手的操作。

5. 裁判员在处理竞赛过程中选手提问的时候，不得单独行动，需要两名以上裁判一起进行处理（裁判不得参入自己选手问题的处理）。

6. 裁判在执裁过程中必须遵守“公正、公开、公平”的竞赛原则，严格按照竞赛技术规则和评分标准进行裁判。裁判员必须按照评分标准的要求操作步骤进行操作，不得对选手的配置做任何修改和调整。如出现不同意见，由各项目裁判小组长召集小组裁判员共同讨论解决，并报备给裁判长裁定。

7. 裁判员应根据技术文件要求做好试题保密工作。同时在大赛组委会正式公布成绩和名次前，裁判员不得对外透露选手的成绩和排名情况。

8. 裁判员在执裁期间，手机等电子产品需统一管理。

9. 裁判员必须按照竞赛的日程安排到岗，不得无故迟到早退、离岗。

10. 裁判员在参加赛前赛题讨论会时要严格遵守会议纪律，会议期间不能携带手机、相机等电子产品对会场进行录音和拍照，不能私自带走比赛讨论资料。

## **（二）选手工作内容**

1. 所有竞赛软件工具由赛场提供；

2. 各参赛队要发挥良好道德风尚，听从指挥，服从裁判，不弄虚作假，如发生弄虚作假者，取消参赛资格，成绩无效；

3. 正式比赛期间，各参赛队领队和其他人员可到赛场观摩，但需要按照赛场的要求在指定地点观摩，并服从现场工作人员的指挥和管理；

4. 各代表队应加强对参赛人员的管理，督促参赛选手要坚决执行竞赛的各项规定，做好赛前准备工作，确保选手带好选手证和允许的比赛自带物品；

5. 在比赛中各参赛队如有异议，可向仲裁组提出申诉，申诉须在比赛后 2 小时内以书面形式交仲裁组。口头报告或其他人员解释处理，仲裁组不予受理。各参赛队不得因申诉或对处理意见不服而停止比赛，否则以弃权处理。仲裁组的决议为最终裁决；

6. 竞赛期间参赛选手不得携带手机等移动通信或上网设备，不得携带移动存储设备、资料等物品；

7. 因设备自身故障导致选手中断竞赛，无法继续比赛的，经确认后由裁判长视具体情况做出裁决；

8. 选手在竞赛过程中不得擅自离开赛场，如有特殊情况，需经裁判同意后作特殊处理，但因此引起的休息、饮水或去洗手间等所消耗的时间计算在竞赛操作时间内；

9. 参赛选手若提前结束竞赛，应向裁判员举手示意，竞赛终止时间由裁判员记录，参赛选手签字确认，结束竞赛后不得再进行任何操



作；

10. 各赛场除现场裁判员、赛场配备的工作人员以外，其他人员未经大赛组委会允许不得进入赛场。

### **（三）问题或争议的处理**

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。

## **五、大赛技术平台**

### **（一）场地基本设备工具清单表**

学号	设备名称	数量	设备要求
----	------	----	------

1	网络空间安全实战平台	1	<p>网络空间安全实战平台</p> <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 100 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，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。</p>
2	PC 机	2	CPU 主频 $\geq 2.8\text{GHZ}$ ， $\geq$ 四核四线程；内存 $\geq 8\text{G}$ ；硬盘 $\geq 256\text{G}$ ；支持硬件虚拟化。
3	强三层交换机	2	

## （二）基本材料清单表

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：

序号	基本材料名称	版本信息
----	--------	------

	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)		Windows XP、Windows 7、Windows 10、Windows Server 2003 及以上版本 (根据命题实际确定)
3	虚拟机安装操作系统 (Linux 系统)		Ubuntu、Debian、CentOS (具体版本根据命题实际确定)
4	其他 主要 应用 软件	VMware workstation	VMware workstation 15 pro 及以上版本免费版
		Putty	Putty 0.67 及以上版本
		Python	Python 3 及以上版本
		Chrome 浏览器	Chrome 浏览器 62.0 及以上版本
		RealVNC 客户端	RealVNC 客户端 4.6 及以上版本

## 六、安全、健康要求

### (一) 健康安全和绿色环保

#### 1. 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);

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

## 2. 选手禁止携带物品

(1) 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：

- (2) 任何储存液体、气体的压力容器；
- (3) 任何有腐蚀性、放射性的化学物品；
- (4) 任何易燃、易爆物品；
- (5) 任何有毒、有害物品；
- (6) 任何没有生产厂商或达不到国家安全标准的工具及设备；
- (7) 任何可能危及安全问题的物品；
- (8) 任何影响竞赛公平性的物品。

## 3. 赛事安全要求

(1) 承办单位应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；

(2) 赛场应具备良好的通风、照明和操作空间的条件；赛场需留有安全通道，必须配备灭火设备；

(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；

(4) 选手、裁判和相关工作人员的防疫工作按组委会执委会要求执行。

## (二) 项目特别规定

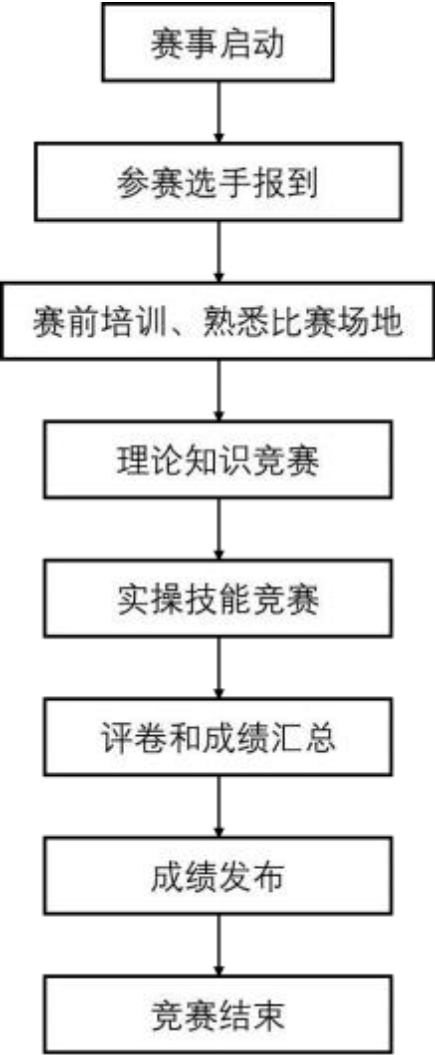
项目特别规定用于提供该赛项所特定的一些细则。项目特别规定包括但不限于：个人 IT 设备、数据存储设备、因特网接入、程序和

工作流程、文档管理和发放。项目特别规定列表：

项目/任务	项目特别规定
使用技术：个人照相机	<b>裁判：</b> 任何情况下，不得携带个人照相机进入竞赛场地中的选手工位，除非由裁判长或裁判长助理批准。 <b>选手：</b> 不得将照相机带入场地
使用技术：移动设备	<b>裁判：</b> 任何情况下，不得携带任何电子设备进入竞赛场地中的选手工位，除非由裁判长批准。 <b>选手：</b> 电子设备（包括移动电话）必须存放在选手背包中（关机或静音）放于储物柜中。任何情况下，不得携带任何电子设备进入竞赛场地中的选手工位，除非由裁判长或裁判长助理批准。
资源文件/笔记	<b>选手：</b> 任何情况下，不得携带笔记进入竞赛场地。在选手竞赛场地工位中记录的笔记必须竞赛期间全程都留在选手桌上。不得将任何笔记带出竞赛场地。
设备故障	<b>选手：</b> 如果出现设备故障，选手必须立即举手通知裁判。裁判应将选手因故障不能操作的时间记录在案。如果设备故障导致的时间损失，将在模块的规定时间之外给予补时。如果设备故障前未能存盘导致的时间损失，不予补时。

七、竞赛流程和日程安排

（一）竞赛流程



（二）竞赛日程安排（以正式发布的比赛指南为准）

日期	时间	事项	参加人员	地点
第 1 天	09:00-13:00	选手报到	工作人员、 参赛队	竞赛场地
第 1 天	14:00-17:00	赛前裁判员培训、 选手熟悉场地	工作人员、 参赛队	竞赛场地

第 2 天	09:00-10:00	理论知识竞赛	参赛选手、 现场裁判	竞赛场地
第 2 天	10:00-13:00	实操技能比赛 竞赛单元 1：CTF 夺旗赛	参赛选手、 现场裁判	竞赛场地
第 2 天	13:00-14:30	实操技能比赛 竞赛单元 2：AWD 攻防赛	参赛选手、 现场裁判	竞赛场地

**八、本竞赛项目的最终解释权归大赛组委会。**