

# 2023 年四川省高职院校大学生 信息安全管理与评估技能大赛竞赛规程

## 一、 赛项名称

赛项名称：信息安全管理与评估

英语翻译：Information Security Management and Evaluation

赛项组别：高职

## 二、 竞赛目的

通过赛项检验参赛选手网络组建、安全架构和网络安全运维管控等方面的技术技能，检验参赛队组织和团队协作等综合职业素养，培养学生创新能力和实践动手能力，提升学生职业能力和就业竞争力。丰富完善学习领域课程建设，使人才培养更贴近岗位实际，实现以赛促教、以赛促学、以赛促改的产教结合格局，提升专业培养服务社会和行业发展的能力，为国家信息安全行业培养选拔技术技能型人才。

## 三、 竞赛内容与时间

### （一）竞赛内容

重点考核参赛选手网络组建、网络系统安全策略部署、信息保护、网络安全运维管理的综合实践能力，具体包括：

1. 参赛选手能够根据大赛提供的赛项要求，设计信息安全防护方案，并且能够提供详细的信息安全防护设备部署拓扑图。
2. 参赛选手能够根据业务需求和实际的工程应用环境，实现网络设备、安全设备、服务器的连接，通过调试，实现设备互联互通。
3. 参赛选手能够在赛项提供的网络设备及服务器上配置各种协议和服务，实现网络系统的运行，并根据网络业务需求配置各种安全策略，以满足应用需求。
4. 参赛选手能够根据网络实际运行中面临的安全威胁，指定安全策略

并部署实施，防范并解决网络恶意入侵和攻击行为。

5. 竞赛总时长为 4 个小时，各竞赛阶段安排如下：

序号	内容模块	具体内容	知识点或技能点
第一 阶段	网络平台搭建	网络规划	VLSM、CIDR 等
		基础网络	VLAN、WLAN、STP、SVI、RIPV2、OSPF、BGP、IPv6、组播等
	网络安全设备配置与防护	访问控制	保护网络应用安全；实现防 DOS、DDOS 攻击；实现包过滤、应用层代理、状态化包过滤、URL 过滤；基于 IP、协议、应用、用户角色、自定义数据流和时间等方式的带宽控制、QoS 策略等
		密码学和 VPN	密码学基本理论、L2L IPSec VPN、GRE Over IPSec、L2TP Over IPSec、IKE：PSK、IKE：PKI、SSL VPN 等
		数据分析	利用日志系统对网络内的数据进行分析、安全管理等
第二 阶段	网络安全事件响应、数字取证调查、应用程序安全	网络安全事件响应	操作系统日志、应用系统/中间件日志、系统进程分析、系统安全漏洞及加固等
		数字取证调查	内存镜像分析、编码转换、加解密、数据隐写、文件分析取证、网络流量包分析等
		应用程序安全	程序逆向分析、移动应用程序代码分析、恶意脚本代码分析等
第三 阶段	网络安全渗透	针对预设的环境进行渗透测试	SQL 注入、文件上传、命令执行、缓冲区溢出、信息收集、逆向文件分析、二进制漏洞利用、应用服务漏洞利用、操作系统漏洞利用、密码学分析等

6. 竞赛分值权重和时间安排

序号	内容模块	竞赛时间
第一阶段 权重 40%	网络平台搭建 权重 15%	240 分钟
	网络安全设备配置与防护 权重 25%	
第二阶段 权重 30%	网络安全事件响应、数字取证调查、应用程序安全 权重 30%	
第三阶段 权重 30%	针对预设的环境进行渗透测试 权重 30%	

## （二）时间安排

本赛项正式比赛时间 4 小时。2023 年 11 月 18 日全天比赛。竞赛时间从 8:00-12:00。如报名队数超过现场设备数量，则分上午、下午两场。下午竞赛时间 13:30-17:30。

## 四、竞赛方式

本赛项为团体赛，以院校为单位组队参赛，不得跨校组队。每所参赛院校至多报 2 支参赛队，每支参赛队由 3 名 2021 级-2023 级同校在籍高职学生（包含非高职高专院校专科阶段学历学生）组成（设队长 1 名），性别不限。每所参赛院校可配指导教师 2 名，指导教师可兼任领队。参加比赛的所有队伍都参与获奖排名，获得国赛资格的学校排名由该校得分最高的队伍决定。

参赛选手在现场根据给定的竞赛任务书，在规定时间内，相互配合实现比赛任务。

## 五、竞赛试题

本赛项采用建立试题库的方式，试题库包括 3 套试题方案。竞赛使用的赛题，将在竞赛前在现场监督人员的监督下，由裁判长随机指定相关人员抽取。

本赛项的命题工作由赛项组委会指定的命题专家组负责，按照竞赛规程的内容要求，在方向和难度上依据教育部颁发的职业院校相关专业人才培养标准和国家职业标准，结合信息安全人才培养要求和信息安全企业岗位需要进行设计，命题专家在完成命题后，交由赛项组委会指定的专家进行审核。

## 六、竞赛规则

1. 参赛资格。参赛选手须为 2023 年在籍高职高专学生（包含非高职院校专科阶段学历学生），报名时每支参赛队由来自同一院校的 3 名选手组成。

2. 参赛选手应严格遵守赛场纪律，服从指挥，着装整洁，仪表端庄，讲文明礼貌。各代表队之间应团结、友好、协作，避免各种矛盾发生。

3. 参赛队的竞赛工位号采用抽签方式确定。赛题以任务书的形式发放，竞赛软件工具在赛前存储在参赛选手的计算机，参赛队根据任务书的要求完成竞赛任务。

4. 参赛选手须提前 20 分钟入场，入场必须佩戴参赛证并出示身份证和学生证。不得私自携带任何竞赛软硬件工具（各种便携式电脑、各种移动存储设备等）、设计资源、通信工具。按工位号入座，检查比赛所需竞赛设备齐全后选手签字方可开始参赛。选手在比赛中应注意随时存盘。迟到超过 10 分钟不得入场。竞赛期间不准出场，竞赛结束后方可离场。

5. 竞赛过程中，各参赛队成员之间可以互相沟通，但不得与任何其它人员讨论问题，也不得向正副主裁判、巡视、裁判员和其他必须进入考场的工作人员询问与竞赛项目的操作流程和操作方法的问题，如有竞赛题目文字不清、软硬件环境等故障的问题时，可向裁判员询问，成员间的沟通谈话不得影响到其他竞赛队伍。

6. 竞赛过程中除正副主裁判、巡视、裁判员和其他必须进入考场的工作人员外，任何其他人员不得进入竞赛场地。

7. 参赛选手要严格遵守竞赛现场规则，如发现有冒名顶替等舞弊行为者，均取消竞赛资格。

8. 竞赛结束（或提前完成）后，参赛队要确认成功提交竞赛要求的文件，裁判员与参赛队队长一起签字确认，参赛队在确认后不得再进行任何操作。

9. 其它未尽事宜，将在赛前向各领队做详细说明。

## 七、竞赛环境

1. 竞赛场地。现场保证良好的采光、照明和通风；提供稳定的水、电和供电应急设备，同时提供所有指导教师休息室1间。

2. 竞赛设备。所有竞赛设备由赛项组委会负责提供和保障，按照参赛队数量准备比赛所需的软硬件平台，详见技术平台部分。

## 八、技术规范

### （一）竞赛项目行业、职业技术标准

竞赛项目的命题结合企业职业岗位对人才培养需求，并参照表中相关国家职业标准制定。

序号	标准号	中文标准名称
1	WSC2022_WSO554_Cyber_Security	《世界技能大赛网络安全项目职业标准》
2	4-04-04-02	《网络与信息安全管理员》
3	4-04-04-04	《信息安全测试员》
4	GB/T 22239-2019	《信息安全技术网络安全等级保护基本要求》
5	GB/T 28448-2019	《信息安全技术网络安全等级保护测评要求》
6	GB/T 36627-2018	《信息安全技术网络安全等级保护测试评估技术指南》
7	GB / T 31509-2015	《信息安全技术信息安全风险评估实施指南》
8	ISO17799	《信息安全管理实施细则》
9	ISO/IEC 27001	《信息安全管理体系》

## (二) 竞赛现场环境标准

1. 竞赛现场设置竞赛区、裁判区、服务区、技术支持区。
2. 竞赛区为参赛队提供标准竞赛设备；竞赛区的每个比赛工位上标明编号；每个比赛区域配置若干工作台，用于摆放计算机和其它调试操作，工作台上摆放制作工具等。
3. 竞赛现场各个工作区配备单相 220V 交流电源。

## (三) 竞赛技术平台标准

赛项组委会提供竞赛平台、网络设备、工作台和计算机及相关工具软件。赛场采用网络安全控制，严禁场内外信息交互。

## 九 技术平台

### (一) 竞赛软件

竞赛组委会提供个人计算机(安装 Windows 操作系统)，用以组建局域网和广域网，并安装常用应用软件。

序号	软件	介绍
1	Windows	操作系统
2	Microsoft Office	文档编辑工具
3	FTP 服务器	设备配置文件上传、下载工具
4	超级终端	设备调试连接工具

竞赛组委会提供服务器环境，配置文档，按照大赛要求提供网络服务。

序号	软件	版本
1	Windows 操作系统	Windows 10 及以上版本
2	Microsoft Office	Microsoft Office 2010 及以上版本
4	VMware Workstation	Version 12 及以上版本
5	Windows Server DataCenter	2016 及以上版本
6	Linux(CentOS)	Version 7.X
7	Ubuntu	20.04

8	Wireshark	3.4.9
9	bind	9.11.4
10	Kali	Version2021.3
11	IDA free	7.0
12	OllyDbg	Version1.10 及以上版本
13	PDF Reader	
14	Volatility	Version2.6 及以上版本
15	Autopsy	Version4.0 及以上版本
16	WinDbg	Version4.0 及以上版本
17	Jadx-gui	1.2.0
18	apktool	2.6.1
19	Android Studio	2021.3.1
20	HxD Hex Editor	Version 2.X 及以上版本
21	Android Emulator	API27
22	StegSolve	1.4
23	audacity	3.1.0
24	Parrot-security	4.11.2
25	gdb-pwndbg	2021.06.22

## (二) 竞赛设备清单

序号	类型	型号	说明
1	三层交换机	神州数码 CS6200-28X	竞赛环境核心交换机
2	防火墙	神州数码 DCFW-1800E-N3002	竞赛出口安全网关
3	web 应用防火墙	神州数码 DCFW-1800-WAF-P	保护 web 服务器不受外界的攻击
4	网络日志系统	神州数码 DCBC-NetLog	记录关键应用的操作人、操作时间，具有很强的不可否
5	堡垒服务器	神州数码 DCST-6000B-Pro	竞赛安全运维的目标平台
6	无线交换机	神州数码 DCWS-6028	管理 AP 设备

7	无线接入点	神州数码 WL8200-I2	无线 AP 接入点
8	POE 供电模块	神州数码 DCWL-PoEINJ-G+	10/100/1000Mbps 单端口 802.3at PoE 模块, 最高输出功率为 30W
9	PC 机	CPU: I5 8 代及以上 主频≥2.0GHZ; 内存: 8GB 及以上	客户机

## 十、评分标准

竞赛评分本着公平公正公开的原则, 评分标准注重对参赛选手价值观与态度、物联网技术应用能力、团队协作与沟通及组织与管理能力的考察。以技能考核为主, 兼顾团队协作精神和职业道德素养综合评定。

## 十一、评分方法

所有参赛代表队评分由裁判委员会统一评定。竞赛评分严格按照公平、公正、公开的原则, 评分标准注重考查参赛选手以下各方面的能力和水平。

序号	内容模块	评分载体	分值	评分方式
第一阶段 权重 40%	网络平台搭建 权重 15%	三层交换机、无线配置文件	15%	结果评分-客观
		网络安全设备配置与防护 权重 25%	防火墙配置截图文件	10%
		流控系统配置截图文件	5%	结果评分-客观
		监控、日志系统配置截图文件	10%	结果评分-客观
第二阶段 权重 30%	网络安全事件响应、数字取证调查、应用程序安全 权重 30%	网络安全事件响应截图文件	10%	结果评分-客观
		数字取证调查截图文件	10%	结果评分-客观
		应用程序安全截图文件	10%	结果评分-客观
第三阶段	网络安全渗透	针对预设的环境进行渗透测	30%	结果评分-客观

权重 30%	权重 30%	试截图文件		
--------	--------	-------	--	--

参赛选手应体现团队风貌、团队协作与沟通、组织与管理能力和工作计划能力等，并注意相关文档的准确性与规范性。

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，提前进行操作或比赛终止后仍继续操作的，由现场裁判负责记录并酌情扣 1-5 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 5-10 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。

4. 设备异常情况处理：参赛选手在竞赛过程中，选手认定设备或器件有故障，可向裁判提出申请，器件或设备经裁判及技术专家组测定完好无故障，则器件或设备认定过程中造成的时间损失由选手所在的小组承担；器件或设备经裁判及技术专家组测定确有故障，则当场更换设备；此过程中（设备测定开始到更换完成）造成的时间损失，在比赛时间结束后，对该小组进行等量的延长比赛时间作为补偿。

#### 5. 违规违纪评判

(1) 对参赛队违规违纪采取“红牌”评判机制，参赛队若违规违纪，由裁判组给予红牌处理，并直接取消该参赛队参赛资格；

(2) 有下列情况之一违规违纪时，直接给予红牌处罚：

- ① 选手因个人因素造成他人人身安全事件和他队设备故障；
- ② 选手在赛场内提出无理要求，并严重干扰赛场秩序；
- ③ 选手在赛场内不尊重赛场规则，有对他人进行人身攻击、言语辱骂

等侵害他人的行为；

- ④ 赛场纪律差,如大声喧哗、不经请示随意走动等；
- ⑤ 携带或使用赛项禁止设备、物品、资料；
- ⑥ 直接或利用技术手段干扰其他参赛队伍竞赛；
- ⑦ 扰乱公平竞赛,偷看他人作答。

## 十二、奖项设定

本赛项奖项设团体奖。竞赛团体奖的设定为：一等奖占比 10%，二等奖占比 20%，三等奖占比 30%。

获得一等奖的参赛队指导教师由组委会颁发优秀指导教师奖证书。

## 十三、赛项安全

### （一）赛项安全规定

1. 赛项举办期间,为保证参赛队的健康及安全,赛项执委会统一安排食宿和各项活动。参赛队如有特殊情况需单独外出或无法参加规定活动,应事先报告赛项执委会,未经赛项执委会批准,参赛队不得单独活动。

2. 竞赛举行期间,参赛选手应严格按照赛场指示的线路进行作业,并服从竞赛裁判员及工作人员的指挥。

### （二）应急处理

1. 赛项举办期间,赛项执委会安排值班人员 24 小时为各参赛队提供应急服务。参赛队如遇特殊情况,可拨打应急电话与赛项执委会值班人员联系。

2. 竞赛举行期间,如发生不可抗力情况,全体人员应服从竞赛工作人员的统一指挥,有序撤离至安全地带。

### （三）医疗服务

承办校医务室安排专人 24 小时值班为参赛队提供医疗服务。

## 十四、申诉与仲裁

## （一）申诉

1. 参赛队对不符合竞赛规定的软硬件设备，有失公正的评判，以及对工作人员的违规行为等，均可提出申诉。

2. 申诉时，应递交由参赛队领队亲笔签字同意的书面报告，报告应对申诉事件的现象、发生的时间、涉及的人员、申诉依据与理由等进行充分、实事求是的叙述。事实依据不充分、仅凭主观臆断的申诉不予受理。

3. 申诉时效：竞赛结束后 1 小时内提出，超过时效将不予受理申诉。

4. 申诉处理：赛场专设仲裁工作组受理申诉，收到申诉报告之后，根据申诉事由进行审查，3 小时内书面通知申诉方，告知申诉处理结果。

申诉人不得无故拒不接受处理结果，不允许采取过激行为刁难、攻击工作人员，否则视为放弃申诉。

## （二）仲裁

1. 组委会下设仲裁工作组，负责受理竞赛中出现的所有申诉并进行仲裁，以保证竞赛的顺利进行和竞赛结果公平、公正。

2. 仲裁工作组的裁决为最终裁决，参赛队不得因申诉或对处理意见不服而停止比赛或滋事，否则按弃权处理。

## 十五、竞赛观摩

在保证竞赛正常进行的前提下，本赛项允许各界人员在指定区域观摩竞赛过程。

观摩人员必须佩戴统一标识，在指定位置进行观摩；观摩过程中，不得与参赛选手进行交流；不得对参赛选手的作业进行评论；为不影响参赛选手进行比赛，观摩人员不得进行拍照或摄影。为保证竞赛的公平与公正，各参赛队领队及指导教师不得观摩本参赛队竞赛过程。

## 十六、竞赛视频

1. 赛项执委会组建赛项报道团队利用多媒体技术及设备录制视频资料，记录竞赛过程，为宣传、仲裁、资源转化提供全面的信息资料。

2. 比赛结束后，对每个参赛工位进行前、后、左、右方位进行拍照，记录完成后的作品状态，为后期申诉和仲裁提供参考依据。

3. 制作优秀选手、指导教师采访，制作裁判专家点评，在规定的网站公布，突出赛项的技能重点和优势特色，扩大赛项的影响力。

## **十七、竞赛须知**

### **（一）参赛队须知**

1. 每个参赛队由 3 名选手组成，选手为 2023 年同校在籍高职学生，不分性别、不分年级，其中队长 1 名。

2. 参赛选手在报名获得确认后，原则上不再更换。如在筹备过程中，选手因故不能参赛，参赛学校主管部门需出具书面说明并按相关参赛选手资格补充人员并接受审核；竞赛开始后，参赛队不得更换参赛选手，允许队员缺席比赛。

### **（二）指导教师须知**

1. 各个参赛队的指导教师不得进入比赛现场指导。

2. 对比赛过程及结果有疑议者，应及时向裁判长书面反映，不得在场外喧哗，影响赛场纪律。

### **（三）参赛选手须知**

1. 参赛选手须认真填写报名表内容，提供个人身份证明，弄虚作假者，将取消比赛资格和成绩。

2. 参赛选手凭大赛组委会颁发的参赛证和有效身份证件（身份证和学生证）参加竞赛及相关活动，参赛队按照赛程安排和规定时间前往指定地点。

3. 参赛选手进入赛场前抽取赛位号，并对抽签结果签字确认。

4. 参赛选手按规定时间进入竞赛场地，对现场条件进行确认并签字，按统一指令开始竞赛。

5. 参赛队须按照竞赛要求提交竞赛结果及相关文件，禁止在竞赛成果

上做任何与竞赛无关的标记。

6. 竞赛结束时间到后，选手不得再进行任何与比赛有关的操作。参赛队若提前结束比赛，应向裁判员举手示意，裁判员记录比赛完成时间。

7. 参赛选手须严格遵守操作规程，确保人身及设备安全。若因选手个人原因出现安全事件或设备故障，由裁判组裁定其竞赛结束，保留竞赛资格，累计其有效竞赛成绩；非选手个人原因出现的安全事件或设备故障，由裁判组做出裁决，可视具体情况给选手补足排除故障耗费时间。

8. 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，参赛队该项成绩为 0 分；如有不服从裁判、扰乱赛场秩序等不文明行为，按照相关规定扣减分数，情节严重的取消比赛资格和成绩。

#### **（四）工作人员须知**

1. 树立服务观念，一切为参赛选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，认真完成本职工作。

2. 工作人员于赛前 60 分钟到达赛场，严守工作岗位，不迟到，不早退，不无故离岗。遇特殊情况需离开岗位，须向赛项执委会请假。

3. 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，按照安全工作预案，组织指挥人员疏散，确保人员安全。

4. 保持通信畅通，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。

5. 竞赛期间，不得在公共场合谈论与竞赛相关事宜，不得与参赛队进行任何形式的交流。