2023年江西省“振兴杯”职业技能大赛

安全防范系统安装维护员项目

技术工作文件

**2023年8月**

**目录**

**1. 项目简介 1**

1.1项目名称 1

1.2项目描述 1

1.3考核目的 1

1.4 相关文件 2

**2. 选手需具备的能力 2**

**3.竞赛项目 13**

3.1 竞赛模块 13

3.2 模块简述 13

3.3命题方式 14

3.5考核时间及地点安排 14

**4.评分标准 14**

4.1 评价分（主观） 14

4.2 机器评分 15

4.3评分流程说明 15

4.4统分方法 15

4.5裁判构成和分组 15

**5.竞赛相关设施设备 17**

5.1场地设备 17

5.2比赛器材 19

**6.选手须知 20**

**7.赛场布局要求 21**

**8.健康安全和绿色环保 21**

8.1环境保护 22

8.2循环利用 22

**9.开放赛场 22**

本项目技术工作文件（技术描述）是对本竞赛项目内容的框架性描述，正式比赛内容及要求以竞赛最终公布的赛题为准。

# 项目简介

## 1.1项目名称

2023年江西省“振兴杯”职业技能大赛——安全防范系统安装维护员。

## 1.2项目描述

该项目所对应的职业工种：安全防范系统安装维护员。

当前，发展信息技术应用创新产业已成为国家战略。信息技术应用 创新发展是国民经济前进的新动能，是贯彻落实建设“网络强国 ”的新举措，是解决安全防护本质问题的根本。

通过举办全省技能竞赛活动，旨在推动信息技术领域安防人才培养，通过“以赛促教、以赛促学、以赛促建、以赛促改”， 引领职业院校专业建设与课程改革，促进产教融合、校企合作，提高院校服务信息技术产业发展的能力。

## 1.3考核目的

为全面贯彻落实习近平总书记对技能人才工作的重要指示精神，更好地在全社会弘扬精益求精的工匠精神。确立培养技能人才的重要性，形成良好的技能人才培养氛围，打造技能成长成才的环境和基础。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。

## 1.4 相关文件

本项目技术工作文件只包含项目技术工作的相关信息。除阅读本文件外，开展本技能项目竞赛还需配合其他相关文件一同使用：

# 选手需具备的能力

参照《信息安全技术网络安全等级保护定级指南》、《信息安全技术信息系统通用安全技术要求》、《信息安全技术网络基础安全技术要求》、《信息安全技术信息系统安全管理要求》，选手应具备的能力包括一下的知识和技能。

|  |
| --- |
| 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。.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.竞赛项目

## 3.1 竞赛模块

|  |  |  |  |
| --- | --- | --- | --- |
| **模块编号** | **模块名称** | **竞赛时间****min** | **分数** |
| **评价分** | **机器评分** | **合计** |
| A | 基础设施设置、安全加固 | 90 | 20 | 0 | 20 |
| B | 安全事件响应、网络安全数据取证、应用安全 | 0 | 40 | 40 |
| C | CTF夺旗攻击 | 90 | 0 | 20 | 20 |
| D | CTF夺旗防御 | 20 | 0 | 20 |
| 总计 | 180 | 40 | 60 | 100 |

## 3.2 模块简述

3.2.1 模块A：基础设施设置、安全加固；模块B：安全事件响应、网络安全数据取证、应用安全

模块A与模块B总分为60分,分为N个任务，每道题的具体分值在赛题中标明；模块A基础设施设置、安全加固部分评分由评分裁判客观评分；模块B安全事件响应、网络安全数据取证、应用安全等部分由系统自动评分和排名，

3.2.2 模块C：CTF夺旗攻击；模块D：CTF夺旗防御

根据竞赛任务书的要求，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。

比赛试题要求答题，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。

## 3.3命题方式

本项目为可以提前公布试题的项目。赛前公布试题（包括赛题、素材、评分细则）。赛前裁判长可结合赛场设备、材料状况，按照本项目试题调整的工作流程和方法，组织裁判人员对已公布的试题进行不超过30%的修改、调整。然后，由裁判长对最终比赛试题签字确认。

## 3.5考核时间及地点安排

本项目2023年江西省“振兴杯”职业技能大赛决赛考核时间为2023年10月，地点：丰城高级技工学校。

# 4.评分标准

本项目评分标准分为机器评分和评价两类。

## 4.1 评价分（主观）

评价分（Judgement）打分方式：2名裁判为一组，各自单独评分，计算出平均权重分，计算出实际得分。

权重表如下：

|  |  |
| --- | --- |
| **权重分值** | **要求描述** |
| 0分 | 各方面均低于行业标准，包括“未做尝试” |
| 1分 | 达到行业标准 |
| 2分 | 达到行业标准，且某些方面超过标准 |
| 3分 | 达到行业期待的优秀水平 |

## 4.2 机器评分

机器评分打分方式：由平台系统对选手提交的答案进行自动评分。

## 4.3评分流程说明

本竞赛的评分方法为结果评分，A、D模块由评分裁判进行评分，B、C模块由平台系统进行自动评分

## 4.4统分方法

赛项最终得分按100分制计分。实际得分采取分项得分、累计总分的计分方式。由裁判长进行复核并统分。总成绩相同时，以B、C模块分数高低进行排序，如果B、C模块分数相同，以最后一个正确答案提交时间排序，先提交者在前。

## 4.5裁判构成和分组

4.5.1 裁判组

本赛项设裁判长1名；加密裁判1名；现场裁判2名，评分裁判2名，共计6人。

4.5.2 裁判任职条件

| 序号 | 裁判 | 专业技术方向 | 执裁经历 | 专业技术职称（职业资格等级） | 人数 |
| --- | --- | --- | --- | --- | --- |
| 1 | 加密裁判 | 电子信息大类相关专业 | 市级及以上赛事执裁经历 | 中级及以上专业技术资格或中级技师职业资格 | 1 |
| 2 | 现场裁判 | 电子信息大类相关专业 | 市级及以上电子信息大类执裁经历 | 中级及以上专业技术资格或中级技师职业资格 | 2 |
| 3 | 评分裁判（含裁判长） | 电子信息大类相关专业 | 省级及以上电子信息大类执裁经历 | 副高及以上专业技术资格或高级技师职业资格 | 3 |

4.5.3 分工方案

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，需要一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。

# 5.竞赛相关设施设备

## 5.1场地设备

竞赛在室内进行，竞赛现场设置场内竞赛区、现场裁判工作区、技术支持区，场外互动区等。

技术支持保障人员在技术支持服务区候场，有需要时在现场裁判的带领下到相关的工位进行赛场技术支持保障。

独立工位的竞赛场地确保参赛队之间互不干扰。每个工位上标明编号，配有一台电脑、一张桌子、一把椅子。

赛场基础设施要求：

（1）工作台内提供有220V交流电源。各工位分区供电，强电弱电分开布线。

（2）采用双路供电；利用UPS防止现场因突然断电导致的系统数据丢失，额定功率：3KVA，后备时间：2小时，电池类型：输出电压：230V±5%V。

（3）竞赛现场符合消防安全规定，现场消防器材和消防栓合格有效，应急照明设施状态合格，赛场明显位置张贴紧急疏散图，赛场出入口专人负责，随时保证安全通道的畅通无阻。

（4）竞赛现场需通风良好、照明需符合教室采光规范。

（5）赛场配备电子监控系统。

竞赛现场具体软硬件需求如下表：

表1：相关设施器材硬件配置参数（每队）

|  |  |  |
| --- | --- | --- |
| 设备名称 | 设备参数 | 数量 |
| 计算机 | 显示器：22英寸（分辨率1920\*1080）及以上键鼠：1套（配鼠标垫）CPU：主频>=2.8GHZ内存：8GB 及以上硬盘：200GB以上 | 2套 |
| U盘 | 16GB及以上容量 | 2个 |

表2：相关设施器材软件配置参数

|  |  |  |
| --- | --- | --- |
| 序号 | 基本材料名称 | 版本信息 |
| 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） | Windows XP、Windows 7、Windows 10、Windows Server2003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 12 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 |
| WPS |  |

注：实际竞赛环境可能不仅限于以上软件

## 5.2比赛器材

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | 数量 | 设备型号 |
| 1 | 网络安全竞赛平台 | 1 | 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、技能内容的竞赛环境实现，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。
 |

# 6.选手须知

（1）.各参赛选手要发扬良好道德风尚，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。

(12).参赛选手若对竞赛过程有异议，在规定的时间内经由领队向赛项仲裁工作组提出书面报告。

**7.赛场布局要求**

竞赛场地划分为检录区、现场服务与技术支持区、休息区、医疗区、观摩通道（视赛场布局进行安排设置）等。

# 8.健康安全和绿色环保

## 8.1环境保护

大赛应注重环境保护，绝不允许破坏环境。

## 8.2循环利用

大赛期间产生的废料必须分类收集和回收。

# 9.开放赛场

赛场开放，公众可在赛场开放区域自由观摩，但不能妨碍选手比赛，不得进入竞赛区域。具体开放视比赛场地布局在赛项说明会另行通知。