# 2024年池州职业技术学院技能大赛
# “信息安全管理与评估”赛项规程

## 一、赛项名称

赛项名称：信息安全管理与评估

英文名称：Information Security Management and Evaluation

赛项组别：高等职业教育

赛项归属：电子信息大类

## 二、竞赛目标

通过赛项检验参赛选手熟悉信息安全行业标准规范和信息安全测试员新职业要求，考查参赛选手网络和信息安全相关的理论知识，重点考查参赛选手信息安全产品配置与应用、网络设备配置与管理、电子数据分析与取证、系统安全评估、网络安全渗透测试等能力，校验参赛队计划组织和团队协作等综合职业素养，强调学生创新能力和实践能力培养，提升学生职业能力和就业质量。

通过大赛引领专业教学改革，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，促进职普融通、产教融合、科教融汇，产教协同培养信息安全领域高素质、专业化、创新型人才。

## 三、竞赛方式与内容

### （一）竞赛方式

本赛项为团体赛，每支参赛队由 3 名选手（设队长 1 名），三个模块比赛同时进行，各模块选手安排由参赛队伍自行安排。参赛选手为 2022、2023 级计算机网络技术和计算机应用技术专业学生以及对信息安全技术感兴趣的其他专业学生等。

**（二）竞赛内容**

参照国赛与省赛的要求，重点考查参赛选手网络和信息安全相关的理论知识，以及信息安全产品配置与应用、网络设备配置与管理、电子数据分析与取证、系统安全评估、网络安全渗透测试等综合实践能力，要求参赛选手能够根据赛项要求，设计信息安全防护方案，实现设备互联互通。重点考核参赛选手网络组建和安全运维、安全审计、网络安全应急响应、数字取证调查、应用程序安全和网络攻防渗透等综合实践能力，具体包括：

1. 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拓扑图。

2. 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. 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，组建网络以满足应用需求。

4. 根据企业所发现的安全事件，展开网络安全事件的调查、分析和取证工作，收集、保存、处理、分析和提供与计算机相关的证据，审计黑客的入侵行为，恢复被黑客破坏的文件。

5.利用一系列网络安全攻击渗透工具对所提供的网络安全攻击靶场环境进行综合分析、挖掘和渗透。

6.网络和信息安全相关的理论技能与职业素养。

**四、竞赛规则**

1.竞赛工位通过抽签决定，竞赛期间参赛选手不得离开竞赛工位。

2.竞赛所需设备、系统软件和辅助工具由组委会统一安排，参赛选手不得自带软件、移动存储、辅助工具、移动通信等违规物品进入竞赛现场。

3.参赛队自行决定选手分工、工作程序和时间安排。

4.参赛队在赛前 10 分钟进入竞赛工位并领取竞赛任务，竞赛正式开始后方可展开相关工作。

5.竞赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和警示。若因选手因素造成设备故障或损坏，无法继续竞赛，裁判长有权决定终止该队竞赛；若因非选手个人因素造成设备故障，由裁判长视具体情况做出裁决。

6.竞赛结束（或提前完成）后，参赛队要确认已成功提交所有竞赛文档，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。

**五、竞赛流程与竞赛范围**

| 序号 | 内容模块 | 具体内容 | 说明 |
|---|---|---|---|
| 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 | 能够利用日志系统对网络内的数据进行日志分析，把控网络安全等； |
| 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 | 参赛队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； |
| | 理论技能与职业素养 | 网络与信息安全理论知识和职业素养 | 信息安全与网络基础、操作系统安全、网络协议安全、网络设备安全、网络数据安全、程序代码安全、网络安全渗透、安全运维与应急服务、密码技术、网络安全法律法规和职业素养等。 |

## 六、评分标准与奖项设置

### （一）制定原则

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：

1.信息安全网络组建能力。

2.信息安全管理的整体内容包括安全运维、安全审计、网络安全应急响应、数字取证调查、应用程序安全和网络攻防渗透能力。

3.相关文档的准确性与规范性。

4.团队风貌、团队协作与沟通、组织与管理能力和工作计划性等。

### （二）评分方法

参赛队成绩由赛项裁判组统一评定；采取分步得分、错误不传递、累计总分的计分方式，分别计算环节得分，不计参赛选手个人得分。

如果总分一样的情况下，优先以第三阶段中的“网络安全渗透”得分进行排名，若第三阶段中的“网络安全渗透”得分相同，以第二阶段得分进行排名，若第二阶段得分相同，以第一阶段得分进行排名。

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，由裁判长按照规定扣减相应分数，情节严重的取消竞赛资格，竞赛成绩记0 分。

### （三）奖项设置

本项目获奖奖项按照“池职院教(2024)9 号”文有关规定进行设置。

## 七、申诉与仲裁

1.赛点组委会设立监督仲裁组，负责竞赛过程中发生的争议和申诉进行最终裁决。

2.参赛队对赛事过程、工作人员工作若有疑义，在事实清楚，证据充分的前提下可向监督仲裁组提出申诉。报告应对申诉事件的现象、发生时间、涉及人员、申诉依据等进行充分、实事求是的叙述。

3.提出申诉应在赛项比赛结束后 1 小时内向监督仲裁组提出。超过时效不予受理。提出申诉后申诉人及相关涉及人员不得离开赛场区域，否则视为自行放弃申诉。

4.监督仲裁组在接到申诉报告后的 1 小时内组织复议，并及时将复议结果以书面形式告知申诉方。监督仲裁组的裁决为最终裁决。

5.申诉方不得以任何理由拒绝接收仲裁结果；不得以任何理由采取过激行为扰乱赛场秩序；仲裁结果由申诉人签收，不能代收；如在约定时间和地点申诉人离开，视为撤诉。

6.申诉方可随时提出放弃申诉。