2018年甘肃省高等职业院校学生技能大赛
“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

赛项组别：高职组

赛项归属产业：第三产业-信息传输、计算机服务和软件业

服务专业：信息安全技术、计算机网络技术及相关专业

承办单位：甘肃交通职业技术学院

二、竞赛目的

（一）检验教学成果

信息安全管理与评估大赛通过赛项检验参赛选手安全网络组建、按照等保要求加固网络系统、安全架构、渗透测试、攻防实战等技术能力，检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。

（二）强化专业建设

针对互联网+、电子政务、智慧城镇和教育信息化等领域信息安全岗位人才急需，按照《高等职业教育电子信息类专业指导规范 Ⅱ》的信息安全与管理专业标准建设框架，通过赛项丰富完善信息安全与管理专业课程体系建设，使人才培养更贴近岗位实际，提升专业培养服务社会和行业发展的能力。

该赛项内容覆盖信息安全与管理专业“信息安全技术与实施”、“信息安全产品配置与应用”、“网络设备配置与管理”、“网络攻防实训”、“系统运行安全与维护”、“操作系统安全配置”、“Web渗透测试

技术”等专业核心课程内容。

（三）促进产教合作

赛项基于信息安全领域主流技术和现行业务流程设计，信息安全行业专家与院校教育专家紧密合作，实现以赛促教、以赛促学、以赛促改的教产融合的赛事创新。

三、竞赛内容

重点考核参赛选手安全网络组建、网络系统安全策略部署、按照等级保护要求进行系统加固与信息保护、网络安全运维管理等综合实践能力，具体包括：

(一) 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拓扑图。

(二) 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。

(三) 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，组建网络以满足应用需求。

(四) 参赛选手能够根据网络实际运行中面临的安全威胁，按照等级要求指定安全策略并部署实施，实现系统的加固，防范并解决网络恶意入侵和攻击行为。

(五) 参赛选手能够按照要求准确撰写工作总结。

(六) 竞赛共分两个阶段，各阶段重点内容如下：

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 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	系统安全攻防及运维安全管控	网络渗透测试及其加固技术	MAC 渗透测试及其加固 DHCP 渗透测试及其加固 ARP 渗透测试及其加固 STP 渗透测试及其加固 VLAN 渗透测试及其加固 路由协议(RIPV2、OSPF)渗透测试及其加固
		操作系统渗透测试及其加固	Windows、Linux 操作系统服务缓冲区溢出渗透测试及其加固
		Web 应用和数据库渗透测试及其加固技术	SQL Injection（SQL 注入）漏洞渗透测试及其安全编程 Command Injection（命令注入）漏洞渗透测试及其安全编程 File Upload（文件上传）漏洞渗透测试及其安全编程 Directory Traversing（目录穿越）漏洞渗透测试及其安全编程 XSS（Cross Site Script）漏洞渗透测试及其安全编程 CSRF（Cross Site Request Forgeries）漏洞渗透测试及其安全编程 Cookie Stole（Cookie 盗用）漏洞渗透测试及其安全编程 Session Hijacking（会话劫持）漏洞渗透测试及其安全编程 配置 WAF（Web 应用防火墙）加固 Web 应用等；

（七）竞赛分值权重和时间分布

序号	内容模块	竞赛时间
第一阶段 权重 60%	网络平台搭建 权重 20%	180 分钟
	网络安全设备配置与防护 权重 40%	
第二阶段 权重 40%	系统安全攻防及运维安全管控 权重 40%	

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，同一学校相同项目报名参赛队不超过 3 支。每支参赛队由 3 名选手（设队长 1 名）和不超过 2 名指导教师组成。

五、竞赛流程

比赛时间限定在 1 天内进行，比赛分为 2 个批次进行，第一批次结束后选手进行封闭，第二批次开考后，第一批次选手方可离开封闭场所。赛项竞赛时间为 3 小时，具体安排如下：

日期	时间	内容	地点	参加人员
4 月 21 日	8:00—12:00	住宿安排	坤怡酒店	参赛队
	14:00	前往学院	坤怡酒店	参赛队
	14:30—15:30	赛项报到	1 教 105-107	参赛队
	15:30—16:30	赛项说明会、第一次抽签	1 教 105-107	参赛队
	16:30—17:30	参观赛场	综合楼五楼（中小型企业网组建实训室）	参赛队
	17:30—19:00	晚餐		
4 月 22 日	6:00—7:00	早餐		
	7:00	乘车前往学院	坤怡酒店	参赛队
	7:30—8:00	参赛队集合、入场	操场	全体人员

日期	时间	内容	地点	参加人员
	8:00—8:30	开赛式	礼堂	参赛队
	8:30—9:00	第二次抽签（第一批）	综合楼五楼（中小型企业网组建实训室）	参赛人员
	9:00—12:00	竞赛（第一批）	综合楼五楼（中小型企业网组建实训室）	参赛人员
	12:00—13:00	午餐		
	13:30—14:00	第二次抽签（第二批）	综合楼五楼（中小型企业网组建实训室）	参赛人员
	14:00—17:00	竞赛（第二批）	综合楼五楼（中小型企业网组建实训室）	参赛人员
	17:30—18:30	晚餐		

六、竞赛赛卷

赛项执委会下设的命题专家组负责本赛项命题工作。

七、竞赛规则

（一）报名资格

参赛选手须为3名2018年度高等职业技术学院全日制在籍学生。参赛选手年龄须不超过25周岁（当年），年龄计算的截止时间以2018年5月1日为准。

（二）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。

（三）竞赛所需的硬件设备、系统软件和辅助工具由赛项执委会统一安排，参赛选手不得自带硬件设备、软件、移动存储、辅助工具、移动通信设备等进入竞赛现场。

（四）参赛队自行决定选手分工、工作程序和时间安排。

（五）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。

（六）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；若因非参赛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。

（七）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。

（八）最终竞赛成绩经复核无误及裁判长、监督长签字确认后，在指定地点，以纸质形式向全体参赛队进行公示。

（九）本赛项最终成绩经赛项裁判长审核无误后签字，承办单位信息员将裁判长确认的电子版赛项成绩信息和纸质打印成绩单报送大赛执委会。

（十）赛项结束后专家工作组根据裁判判分情况，分析参赛选手在比赛过程中对各个知识点、技术的掌握程度，并将分析报告报备大赛执委会办公室，执委会办公室根据实际情况适时公布。

（十一） 赛项每个比赛环节裁判判分的原始材料和最终成绩等结果性材料经监督组人员和裁判长签字后装袋密封留档，并由赛项承办院校封存，委派专人妥善保管。

八、竞赛环境

竞赛工位内设有操作平台，每工位配备 220V 电源，工位内的电缆线应符合安全要求。每个竞赛工位面积≥6 ㎡，确保参赛队之间互不干扰。竞赛工位标明工位号，并配备竞赛平台和技术工作要求的软、硬件。环境标准要求保证赛场采光(大于 500lux)、照明和通风良好。

九、技术规范

该赛项涉及的信息网络安全工程在设计、组建过程中，主要有以下7项国家标准，参赛队在实施竞赛项目中要求遵循如下规范：

序号	标准号	中文标准名称
1	GB 17859-1999	《计算机信息系统安全保护等级划分准则》
2	GB/T 20271-2006	《信息安全技术信息系统通用安全技术要求》
3	GB/T 20270-2006	《信息安全技术网络基础安全技术要求》
4	GB/T 20272-2006	《信息安全技术操作系统安全技术要求》
5	GB/T 20273-2006	《信息安全技术数据库管理系统安全技术要求》
6	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》
7	GB/T 20269-2006	《信息安全技术信息系统安全管理要求》
8	ISO OSI	OSI 开放系统互连参考模型
9	IEEE 802.1	局域网概述，体系结构，网络管理和性能测量
10	IEEE 802.2	逻辑链路控制 LLC
11	IEEE 802.3	总线网介质访问控制协议 CSMA/CD 及物理层技术规范
12	IEEE 802.6	城域网（Metropolitan Area Networks)MAC 介质访问控制协议 DQDB 及其物理层技术规范
13	IEEE 802.10	局域网安全技术标准
14	IEEE 802.11	无线局域网的介质访问控制协议 CSMA/CA 及其物理层技术规范
15	GB/T 22239-2008	信息安全技术信息系统安全等级保护基本要求

十、技术平台

(一) 竞赛软件

赛项执委会提供个人计算机（安装 Windows 操作系统），用以组建竞赛操作环境，并安装 Office 等常用应用软件。

序号	软件	介绍
1	Windows	操作系统
2	Microsoft Office	文档编辑工具
3	VMware	虚拟机运行环境
4	超级终端	设备调试连接工具

赛项执委会提供渗透测试机和靶机虚拟机环境。

序号	软件	介绍
1	Windows 7\Windows XP	Windows 客户机操作系统
2	Windows Server 2003\2008	Windows 服务器操作系统

3	Ubuntu\Debian	渗透测试机操作系统
4	Linux CentOS	Linux 服务器操作系统

（二）竞赛设备清单

序号	设备名称	数量	参考型号
1	三层虚拟化交换机	1	神州数码 CS6200 交换机
2	防火墙	1	神州数码 DCFW-1800E-N3002
3	堡垒服务器	1	神州数码 DCST-6000B
4	WEB 应用防火墙	1	神州数码 DCFW-1800-WAF-LAB
5	网络日志系统	1	神州数码 DCBI-NetLog-LAB
6	无线交换机	1	神州数码 DCWS-6028
7	无线接入点	1	神州数码 WL8200-I2
8	PC 机	3	多核 CPU，CPU 主频>=3.5GHZ,>=四核心八线程，内存>=8G，具有串口或者配置 USB 转串口的配置线，支持硬件虚拟化

十一、成绩评定

（一）裁判工作原则

按照《2018 年全国职业院校技能大赛专家和裁判工作管理办法》建立职业院校技能大赛赛项裁判库，裁判长由赛项执委会向大赛执委会推荐，由大赛执委会聘任。赛前建立健全裁判组。裁判组为裁判长负责制，划分裁判小组（2 人为一组），并设有专职督导人员 1-2 名，负责比赛过程全程监督，防止营私舞弊。

（二）裁判评分方法

裁判组负责竞赛机考评分和结果性评分，由裁判长负责竞赛全过程；裁判员提前报到，报到后所有裁判的手机全部上缴裁判长统一保管，评分结束返回，保证竞赛的公正与公平。

竞赛现场有监督员、裁判员、监考员、技术支持队伍等组成，分工明确。根据现场环境，每位监考员负责 2-3 组参赛队，2-3 名技术

支持工程师负责所有工位设备应急。监考员负责与参赛队伍的交流沟通及试卷等材料的收发，裁判员负责设备问题确认和现场执裁，技术支持负责执行裁判确认后的设备应急处理。

（三）成绩产生办法

裁判员执裁过程中，各模块由分组裁判员进行背对背评分，由小组长负责裁定成绩一致方提交到成绩统计组，统计组再次核对每小题的得分，并汇总产生每套竞赛文档号的对应成绩。

裁判长正式提交竞赛文档号对应的评分结果并复核无误后，在监督人员监督下对形成成绩一览表，成绩表由裁判长、监督员签字确认。

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：

竞赛阶段	竞赛任务	考核内容	分值	评分方式
第一阶段 权重 60%	网络平台搭建 权重 20%	网络规划文档	10%	结果评分-客观
		按照等保要求进行网络设备配置,提交相关配置文件或截图文件	10%	结果评分-客观
	网络安全设备配置与防护 权重 40%	防火墙相关配置截图文件	40%	结果评分-客观
		网络日志系统相关配置截图文件		结果评分-客观
		web 应用防火墙相关配置截图文件		结果评分-客观
		无线控制器相关配置文件		结果评分-客观
		三层交换机相关配置文件		结果评分-客观
第二阶段 权重 40%	系统安全攻防及运维安全管控 权重 40%	服务器加固配置	20%	机考评分
		服务器渗透配置	20%	机考评分

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。

(四) 成绩复核与公布

1. 为保障成绩评判的准确性，监督组将对赛项总成绩排名前 30%的所有参赛队伍(选手)的成绩进行复核；对其余成绩进行抽检复核，抽检覆盖率不得低于 15%。如发现成绩错误以书面方式及时告知裁判长，由裁判长更正成绩并签字确认。复核、抽检错误率超过 5%的，裁判组将对所有成绩进行复核。

2. 竞赛成绩已复核无误后，经项目裁判长、监督人员审核签字后确定，并在赛场及赛场外张贴纸质成绩进行公示。

十二、申诉与仲裁

（一）申诉

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

2. 申诉应在竞赛结束后 1 小时内提出，超过时效不予受理。申诉时，应按照规定的程序由参赛队领队向赛项仲裁工作组递交书面申诉报告。报告应对申诉事件的现象、发生的时间、涉及到的人员、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将不予受理。申诉报告须有申诉的参赛选手、领队签名。

3.赛项仲裁工作组收到申诉报告后，应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。

4.申诉人不得采取过激行为刁难、攻击工作人员，否则视为放弃申诉。

（二）仲裁

赛项设仲裁工作组接受由代表队领队提出的对裁判结果等方面问题的申诉。赛项仲裁工作组在接到申诉后的2小时内组织复议，并及时反馈复议结果。仲裁工作组的仲裁结果为最终结果。