

2018 年学院竞赛月

“可信华泰”杯信息安全管理与评估赛项竞赛规程

一、赛项名称

赛项名称：“可信华泰”杯信息安全管理与评估

赛项组别：院级

赛项归属产业：信息安全

二、竞赛目的

中央网络安全与信息化办公室[2016]4号文件,联合国家发改委、教育部、科技部、工信部、人社部发文鼓励信息安全人才培养,从教材编写、实验室建设等多个环节加以提升。面对市场对安全人才的大量需求,传统的学院派缺少企业引入行业应用经验,也缺乏系统全面的安全建设课程与实践。故希望通过赛项培养和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,以及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

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、攻防平台的连接，通过调试，实现学生终端设备与竞赛设备的互联互通。

3. 参赛选手能够在赛项提供的网络设备及安全设备、攻防平台上配置各种协议和策略，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，实现安全设备的策略配置，并根据竞赛题目要求进行解题获得相关答案。

5. 参赛选手能够按照解决报告模板要求准确填写并提交。

6. 以参赛队为单位进行分组答题。

7. 竞赛总时长为 2 个小时，第一阶段为所有参赛队进行理论竞赛，时间为 30 分钟，第二阶段为所有参赛队进行比赛，竞赛时间为 1 小时 30 分钟，各竞赛阶段安排如下：

序号	内容模块	具体内容	说明
第一阶段	理论竞赛	网络基础及信息安全基础	能够掌握基本的相关理论知识
第二阶段	网络安全设备配置与防护	防火墙技术配置	能够在局域网中配置防火墙，策略路由配置、NAT 配置、访问控制策略配置等；
		WEB 防御技术配置	能够配置漏扫防护策略，包括 SQL 注入防护、弱密码防护配置；
		数据库审计技术配置	能够利用数据库系统对网络内的数据进行分析，把控网络安全。
第三阶段	系统安全攻防及运维安全管控	服务器渗透技术	针对未设置防护的数据库和服务进行扫描、密码猜测等渗透测试。
		服务器加固技术	强制访问控制、数据保护、行为审计等

8. 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%	理论竞赛	30 分钟
第二阶段 权重 40%	网络安全设备配置与防护	90 分钟
第三阶段 权重 20%	系统安全攻防及运维安全管控	

四、竞赛方式

本赛项为团体赛，以个人自由组队参赛。每支参赛队由 2-3 名选手组成。

参赛选手须为我院全日制在籍学生，性别不限。

五、竞赛流程

比赛限定在 1 天内进行，赛项竞赛时间为 2 小时，时间为 13:30-16:35，具体安排如下：

日程安排	
13:20	裁判进入裁判室
13:30-14:00	指导老师抽签，学生理论竞赛
14:00-14:05	参赛队就位，宣读竞赛纪律
14:05-14:10	学生准备开赛
14:10-15:40	学生竞赛结束
15:45-16:30	评分

备注：第一阶段和第二阶段赛题在开始比赛时同时发放，并于 13:30 统一提交答题成果，交卷完毕后发放第三阶段赛题。

六、竞赛赛题

1. 赛项执委会下设的命题专家组负责本赛项命题工作。
2. 赛项命题分为两部分，理论部分和实操部分，理论部分题目

内容主要包括网络安全基础知识、防火墙设置、可信计算、路由交换的设置、服务器搭建、linux 命令等，实操部分包含系统安全攻防及运维安全管控、系统加固、系统攻防，题目涉及渗透测试、web 应用程序安全攻防、数据库注入测试及其加固、网络协议渗透测试及其加固等。

七、竞赛规则

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。

1. 竞赛所需的硬件设备、系统软件和辅助工具由组委会统一安排，参赛选手不得自带硬件设备、软件、移动存储、辅助工具、移动通信等进入竞赛现场。

2. 参赛队自行决定选手分工、工作程序和时间安排。

3. 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。

4. 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。

5. 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、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 $\geq 6\text{ m}^2$ ，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;每支参赛队提供一个垃圾箱。

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》

十、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,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	浏览器	火狐浏览器、谷歌浏览器

竞赛组委会提供服务器环境,按照大赛要求提供网络服务。

序号	软件	介绍
1	Windows 7	服务器操作系统
2	Windows Server 2003	服务器操作系统
3	Linux Debian	服务器操作系统

(二) 竞赛设备清单

序号	类型	型号	数量	说明
1	三层交换机	H3C	1	竞赛环境核心交换机

		LS-5130-52S-SI		
2	下一代防火墙	深信服 AF-1000-A400	1	竞赛出口安全网关
3	信息安全风险评估平台	天镜脆弱性扫描与管理系统	1	扫描服务器漏洞，不受外界的攻击
4	数据库安全实验平台	安华金和 数据库监控与审计系统	1	数据库漏洞攻击监测，根据敏感语句、sql 注入、漏洞攻击、风险操作等统计数据库信息。
5	攻防平台	可信华泰 HTTC-NRT	1	攻防操作仿真平台

十一、成绩评定

（一）裁判工作原则

赛前建立健全裁判组。裁判组由裁判长负责制，划分裁判小组（2人为一组），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、技术支持队伍等组成，分工明确。根据现场环境，每位监督员负责 2-3 组参赛队，5-6 名技术支持工程师负责所有工位设备应急。监督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題的得分，并汇总产生每套竞赛文档号的对应成绩。

裁判长在竞赛结束 2 小时内提交竞赛文档号对应的评分结果，经

复核无误，由裁判长、监督人员和仲裁人员签字确认后公布。

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，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：

序号	内容模块	评分载体	分值	评分方式
第一阶段 权重 40%	理论竞赛权重 40%	理论竞赛答题	40%	机考评分
第二阶段 权重 40%	网络安全设备配置与防护 权重 40%	防火墙配置截图文件	20%	人工评分
		Web 安全防护系统配置截图文件	10%	人工评分
		网络日志系统配置截图文件	10%	人工评分
第三阶段 权重 20%	系统安全攻防及运维安全管控 权重 20%	服务器加固配置截图文件	10%	人工评分
		服务器渗透配置截图文件	10%	人工评分

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。

十二、奖项设定

赛设一等奖、二等奖、三等奖、优秀奖。获奖比例分别为该项目参赛人数的 5%、10%、15%、30%。

十三、赛项安全

赛事安全是技能大赛一切工作顺利开展的先决条件，是本赛项筹备和运行工作必须考虑的核心问题。

（一）组织机构

赛项执委会组织专门机构负责赛区内赛项的安全工作，保证比赛安全，制定应急预案，及时处置突发事件。制定相应安全管理的规范、流程和突发事件应急预案，全过程保证比赛筹备和实施工作安全。

（二）赛项设计

1. 比赛内容涉及的器材、设备应符合国家有关安全规定。赛项专家组应充分考虑比赛内容和所用器材、耗材可能存在的危险因素，通过完善设计规避风险，采取有效防范措施保证选手备赛和比赛安全。危险提示和防范措施应在赛项技术文件中加以明确。

2. 赛项技术文件应包含国家（或行业）有关职业岗位安全的规范、条例和资格证书要求等内容。

3. 赛项执委会须在赛前对本赛项全体裁判员进行裁判培训和安全培训，对服务人员进行安全培训。源于实际生产过程的赛项，须根据《中华人民共和国劳动法》等法律法规，建立完善的安全事故防范制度，并在赛前对选手进行培训，避免发生人身伤害事故。

4. 赛项执委会须制定专门方案保证比赛命题、赛题保管和评判过程的安全。

（三）比赛环境

1. 环境安全保障

赛场组织与管理员应制定安保须知、安全隐患规避方法及突发事件预案，设立紧急疏散路线及通道等，确保比赛期间所有进入竞赛地点的车辆、人员需凭证入内；严禁携带易燃易爆物、管制刀具等危险品及比赛严令禁止的其他物品进入场地；对于紧急发生的拥挤、踩踏、地震、火灾等进行紧急有效的处置。

2. 信息安全保障

安装 UPS：采用 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；市电采用双路供电。

3. 操作安全保障

赛前要对选手进行计算机、网络设备、工具等操作的安全培训，进行安全操作的宣讲，确保每个队员能够安全操作设备后方可进行比赛。裁判员在比赛前，宣读安全注意事项，强调用火、用电安全规则。

4. 赛项执委会须在赛前组织专人对比赛现场进行考察，并对安全工作提出明确要求。赛场的布置，赛场内的器材、设备，应符合国家有关安全规定。如有必要，也可进行赛场仿真模拟测试，以发现可能出现的问题。赛前须按照赛项执委会要求排除安全隐患。

5. 赛场周围要设立警戒线，防止无关人员进入发生意外事件。比赛现场内应参照相关职业岗位要求为选手提供必要的劳动保护。在具有危险性的操作环节，裁判员要严防选手出现错误操作。

6. 对于比赛内容涉及大用电量、易发生火灾等情况的赛项，必须明确制度和预案，并配备急救人员与设施。

7. 赛项执委会须会同承办单位制定开放赛场和体验区的人员疏导方案。赛场环境中存在人员密集、车流人流交错的区域，除了设置

齐全的指示标志外，须增加引导人员，并开辟备用通道。

8. 大赛期间，赛项承办单位须在赛场管理的关键岗位，增加力量，建立安全管理日志。

9. 参赛选手进入赛位、赛事裁判工作人员进入工作场所，严禁携带通讯、照相摄录设备，禁止携带记录用具。如确有需要，由赛场统一配置、统一管理。赛项可根据需要配置安检设备对进入赛场重要部位的人员进行安检。

（四）组队责任

1. 各参赛队须加强参赛人员的安全管理，实现与赛场安全管理的对接。

2. 参赛队组成后，须制定相关管理制度，并对所有选手、指导教师进行安全教育。

（五）应急处理

比赛期间发生意外事故，发现者应第一时间报告赛项执委会，同时采取措施避免事态扩大。赛项执委会应立即启动预案予以解决并向赛区执委会报告。出现重大安全问题的赛项可以停赛，是否停赛由赛区组委会决定。事后，赛区执委会应向大赛执委会报告详细情况。

十四、申诉与仲裁

在比赛过程中若出现有失公正或有关人员违规等现象，参赛队可在比赛结束后 2 小时之内向仲裁组提出书面申诉。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。

十五、竞赛观摩

竞赛环境依据竞赛需求和职业特点设计，在竞赛不被干扰的前提下安全开放部分赛场。观摩人员需佩戴观摩证件在工作人员带领下沿

指定路线、在指定区域内到现场观赛。

十六、竞赛须知

（一）参赛队须知

1. 各参赛队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. 各参赛队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料。

3. 竞赛过程中，除参加当场次竞赛的选手、执行裁判员、现场工作人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。

4. 参赛队若对竞赛过程有异议，在规定的时间内由领队向赛项仲裁工作组提出书面报告。

5. 对申诉的仲裁结果，参赛队要服从和执行。参赛选手不得因申诉或处理意见不服而停止竞赛，否则以弃权处理。

（二）参赛选手须知

1. 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。

2. 参赛选手需持统一印制的参赛证和有效身份证件参加竞赛。

3. 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。

4. 参加选手请勿携带与竞赛无关的电子设备、通讯设备及其他资料与用品进入赛场。

5. 参赛选手应按照规定时间抵达赛场，凭参赛证、身份证件检录，按要求入场，不得迟到早退。

6. 参赛选手应增强角色意识，科学合理分工与合作。

7. 参赛选手应按有关要求在指定位置就坐。

8. 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，只是操作无法继续的，经项目裁判长确认，予以启用备用计算机。

9. 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。

10. 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。

11. 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。

12. 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。

（三）评分人员须知

1. 评分采用手工评分和计算机系统自动评分相结合的方式。

2. 评分人员要认真阅读评分细则，严格执行评分标准，准确量分。

3. 评分人员要严格按照评分细则的规定评分，及时、准确地将评分结果记录在相应的评分登记表中，并签名。

4. 评分人员在评分过程中存在疑问时，应及时向项目裁判长咨询。

5. 评分人员在评分过程中发现的试卷问题，应及时向项目裁判员报告。

6. 计算机系统自动评分部分的分值设置要与评分标准和评分细则一致。

7. 计算机内所有参赛队分值设置均为零，无基础分值。

（四）工作人员须知

1. 树立服务观念，一切为选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，在赛项执委会的领导下，按照各自职

h2. 所有工作人员必须佩带证件，忠于职守，秉公办理，保守秘密。

3. 注意文明礼貌，保持良好形象，熟悉赛项指南。

4. 自觉遵守赛项纪律和规则，服从调配和分工，确保竞赛工作的顺利进行。

5. 提前 30 分钟到达赛场，严守工作岗位，不迟到，不早退，不得无故离岗，特殊情况需向工作组组长请假。

6. 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，按照应急预案，组织指挥人员疏散，确保人员安全。

7. 工作人员在竞赛中若有舞弊行为，立即撤销其工作资格，并严肃处理。

8. 保持通讯畅通，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。