**2018年全国职业院校技能大赛**

**赛项申报书**

赛项名称：网络空间安全

赛项类别：常规赛项■ 行业特色赛项□

赛项组别：中职组■ 高职组□

涉及的专业大类/类：信息技术类

方案设计专家组组长：

手机号码：

方案申报单位（盖章）：中国职业技术教育学会

 创业教育专业委员会

方案申报负责人：

方案申报单位联络人：

联络人手机号码：

电子邮箱：

通讯地址：

邮政编码：

申报日期：2017年8月30日

**2018年全国职业院校技能大赛**

**赛项申报方案**

**一、赛项名称**

（一）赛项名称

网络空间安全

（二）压题彩照

图：2017年网络空间安全国赛现场

（三）赛项归属产业类型

第三产业-信息传输、计算机服务和软件业

（四）赛项归属专业大类/类

09信息技术类

中职新版专业目录将新增专业：网络信息安全专业

090500计算机网络专业

090100计算机应用专业

090600网站建设与管理专业

**二、赛项申报专家组**

**三、赛项目的**

没有网络安全就没有国家安全，网络空间安全已经上升到国家安全战略高度。当今世界，信息技术革命日新月异，对国际政治、经济、文化、社会、军事等领域发展产生了深刻影响。信息化和经济全球化相互促进，互联网已经融入社会生活方方面面，深刻改变了人们的生产和生活方式。我国正处在这个大潮之中，受到的影响越来越深。我国互联网和信息化工作取得了显著发展成就，网络走入千家万户，网民数量世界第一，我国已成为网络大国。

与此相对应的是，我国网络空间安全问题频出，损失巨大。中国是网络攻击的主要受害国。侵犯个人隐私、损害公民合法权益等违法行为时有发生。2014年，中央网络安全和信息化领导小组宣告成立，表明加强网络安全和信息化建设已经摆在国家发展战略的重要位置。2017年6月1日，《中华人民共和国网络安全法》正式施行，护卫我国的“第五疆域”。

全国职业院校技能大赛举办10年以来，赛项设置一直强调与产业结构升级和高新技术发展同步，2017年中职组“网络空间安全”赛项的举办直接促进了相关院校“网络信息安全”专业的设立。

2017年7月8日，全国工业和信息化职业教育教学指导委员会暨中职信息技术类相关专业目录修订启动会议在北京召开。会上发布了《专业设置优化调整建议报告》，报告中提出新增 “网络信息安全”专业，与“计算机网络技术”并列。7月23日，全国工业和信息化职业教育教学指导委员会中等职业信息技术类计算机相关专业目录修订统稿会议在广州召开，会上确定了《网络信息安全专业简介》和《网络信息安全专业论证分析》。

2017年8月，中央网络安全和信息化领导小组办公室秘书局、教育部办公厅印发《一流网络安全学院建设示范项目管理办法》，贯彻习总书记关于“下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院”的重要指示精神，中央网信办、教育部决定在2017年至2027年期间实施一流网络安全学院建设示范项目。将网络和信息安全教育教学和人才培养推上了一个新高度。

因此，本赛项是践行“以赛促学、以赛促教、以赛促改、以赛促创”的典型案例。

**四、赛项设计原则**

（一）公开、公平、公正。

本赛项严格遵守大赛制度，开赛前一个月全部公开赛题，赛题以赛项专家组、国家示范校、行业专家、企业专家为班底成立题库开发团队，参照行业规范，工作内容，设计技能操作以及高职信息安全赛项内容进行分析整理，确定适合中职学生的赛题。并将及时更新相关规程、评分细则，并在大赛官方网站上进行发布。

在赛制设计中，本赛项全部分数由计算机评测系统自动评分，大屏幕实时滚动并显示得分情况，最大程度保证赛项公开透明。在2017年的比赛中，赛项进行了现场直播，效果逼真，通过扫描二维码实现全国手机用户实时观看，实时显示选手得分和排名，赛后多数选手根据自己得分就可以推算出名次。可以说，本赛项是国赛中少有的全公开赛项。

（二）常规赛项关联专业人才需求量大或职业院校开设专业点多，服务国家重点战略。

网络安全是国家战略。当前中国重要行业信息系统和信息基础设施需要各类网络信息安全人才以每年1.5万人的速度递增，到2020年相关人才需求将增长到140万。7.3亿中国网民的网络安全问题，已成为行业乃至国家亟待解决的问题。巨大的市场需求，使信息安全技术应用与网络安全管理人才变得炙手可热，中等职业学校可以着重于网络安全产品应用与维护、计算机网络及系统的安全管理与维护领域的人才培养，以运维类岗位为目标，培养具有良好职业道德，熟悉网络与信息安全方面的法律法规，能从事网络、系统、数据、应用安全维护和管理能力的高素质技能型人才。

适合中职学生的职业岗位：网络安全管理员、系统安全管理员、网站安全管理员、信息系统运行维护工程技术人员、网络与信息安全管理员、信息通信信息化系统管理员。通过自主发展能够胜任的岗位：信息安全产品技术支持、信息安全产品测试员、信息安全产品销售员、信息安全产品集成与售后服务等。

本赛项涉及的专业点也较多，在信息技术类专业中，非常匹配的专业就有：新专业网络信息安全专业、090500计算机网络专业、090100计算机应用专业、090600网站建设与管理专业。还有几个专业譬如：090700网络安防系统安装与维护、090800软件与信息服务、090900客户信息服务等专业，现在也需要有信息安全的必要技能才能更好地就业。因此网络空间安全是一个具有广泛参与度的赛项。

（三）竞赛内容对应相关职业岗位或岗位群、体现专业核心能力与核心知识、涵盖丰富的专业知识与专业技能点。

赛项设计面对的岗位很多，譬如《中华人民共和国职业分类大典（2015年版）》中明确列举的就有：2-02-10-24 计算机网络工程技术人员，2-02-10-07 信息安全工程技术人员，2-02-10-08 信息系统运行维护工程技术人员，4-04-04-02 网络与信息安全管理员，4-04-04-03 信息通信信息化系统管理员等，人才需求量大。

赛项设计适应国家“新一代信息技术产业”的需要，聚焦计算机网络工程领域岗位的主要技能，与相关企业紧密合作，以实际工程项目为基础，基于工作过程，针对计算机网络专业学生的“能力短板”，围绕计算机网络工程领域的先进技术、主流产品，力求突出工程实践；着重考查选手的安全意识、工程能力、职业道德、组织管理能力、工作计划性和职业素养，以赛促教，以赛促改，引领计算机网络专业的教育教学改革；通过竞赛提升中职信息技术相关专业学生的网络安全意识和设备配置能力，使之具备风险评估的基本能力；通过竞赛展示中职学生的工程实践能力，促进社会对网络安全工程相关岗位的了解，提高中职学校的社会认可度，提高学生的就业质量和就业水平。

（四）竞赛平台成熟。根据行业特点，赛项选择相对先进、通用性强、社会保有量高的设备与软件。

本赛项在国赛、省赛或行业技能竞赛中已成功举办两届以上。本赛项使用的竞赛平台广泛应用于中高职技能大赛、各地省赛以及行业竞赛，如：全国职业院校技能大赛，江苏、浙江、安徽、河南、广东、北京、上海、青岛等20多个省市级技能大赛等。平台技术成熟，功能稳定，性能出色，赛题课件在设计中注重中职学生特点。

**五、赛项方案的特色与创新点**

竞赛内容方面：结合实际工作，基于工作过程，模拟实战演练，考察选手在网络、系统、攻防各个领域的综合能力，尤其是攻防环节，各选手同时互相攻守的过程在大屏幕上实时显示，极具观赏性；

竞赛过程安排：比赛过程充分考虑实际工作，分为两个阶段进行比赛，既有传统的系统搭建和维护内容，也有经典的系统安全渗透测试，最后采用全场的全攻全守，难度逐渐增加，节奏清晰，符合认知规律。

竞赛结果评判：全部分数由计算机评测系统自动且实时评分，分数直播公开，保证比赛公开、公平性。对于场外的指导教师而言，能够清楚了解到自己选手的竞赛状态，了解得失，利于后期复盘，总结提高，用于教学。对于赛项的推广，以赛促教、促学的意义重大；

竞赛资源转化：结合教育部[国家级职业教育专业教学资源库项目](http://www.baidu.com/link?url=6tykEFj6JXmWjsSbS4LzvrQjv1Hg_DO5-zZYGV741bKFQN1cvCPFUF-8rArEzRaq)-信息安全资源库建设项目，中高职衔接，以赛促改，推进竞赛成果向教学资源转化。通过教产合作，重视成果转化，推进竞赛成果向教学资源转化开发，促进教学改革和专业建设，同时完善中职学校网络信息安全专业教学体系，计划配套多本教材，设计新的交互式仿真实训课件辅助教学，通过竞赛将人才供需双方关联起来。

**六、竞赛内容简介（须附英文对照简介）**

赛项名称：网络空间安全

赛项简介：面向中职信息技术类专业的学生，注重考核网络安全设计、安全策略配置、系统渗透测试以及信息安全攻防等方面，还原实际工作场景，基于工作过程的竞赛任务书设计，考察选手网络空间安全的综合技能和素质。

Competition Name : [Cyberspace Security](http://www.baidu.com/link?url=azUPQZL-A0FvevJa1d9wi4L8c-fCEXe6jdt4y3it9ek3yx2R4lqOOfdGsXoXIk4h0xxl6NxkP0VkZRstocqjnb-orjtnDUv__SaJYzGbZWSG3HEDrA5FIUyL14IW1QdC) [Competition](http://www.baidu.com/link?url=I_NP-qi0YdumxWDz2Tay-4LRQxIGJyRs_XjJV_TjztqW_88_JbKe_NDEKiD16HhtB9UZQtHtN8-evANS1X52p2uFIAD0Tip8FTRKjSnxK5S)

Brief Introduction: Aimed at information technology students in secondary vocational schools, this contest is based on the working process of the contest task design to investigate the contestants’ comprehensive skills and qualifications for cyberspace security.

By simulating actual working environment we focus on the assessment of the design of network security, security policy configuration, system penetration test, and information security attack and defense.

**七、竞赛方式（含组队要求、是否邀请境外代表队参赛）**

本赛项为团体赛，每支参赛队限2名同校选手，不得跨校组队。同一学校报名参赛队不超过1支。每队限报 2 名指导教师，指导教师须为本校专兼职教师。

参赛选手须为中等职业学校全日制在籍学生或者五年制高职一至三年级（含三年级）的学生。参赛选手年龄须不超过 21 周岁，年龄计算的截止时间以比赛当年的5月1日为准。凡在往届全国职业院校技能大赛本项目获一等奖的选手，不能再参加本项目的比赛。

由各省、自治区、直辖市、计划单列市组织报名参加。为鼓励各省积极组织省赛，对于组织相应赛项省级选拔赛并经大赛执委会审查备案的省份，由大赛执委会根据赛项特点及承办单位实际承接能力，在条件许可的情况下可增加1支参赛队。

本赛项正在与国际参赛队接洽，同时欢迎国内外团队及选手到场观赛。

**八、竞赛时间安排与流程**

（一）竞赛日程

比赛限定在1天内进行，比赛场次为1场，赛项竞赛时间为3小时，时间为9:00-12:00，具体安排如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **日期** | **时间** | **事项** | **参加人员** | **地点** |
| 竞赛前2日 | 20:00前 | 裁判、仲裁、监督报到 | 工作人员 | 住宿酒店 |
| 竞赛前1日 | 09:00-12:00 | 参赛队报到，安排住宿，领取资料 | 工作人员、参赛队 | 住宿酒店 |
| 09:00-12:00 | 裁判工作会议 | 裁判长、裁判员、监督组 | 会议室 |
| 13:00-14:30 | 领队会 | 各参赛队领队、裁判长 | 会议室 |
| 15:00-16:00 | 参观赛场 | 各参赛队领队 | 竞赛场地 |
| 16:00 | 检查封闭赛场 | 裁判长、监督组 | 竞赛场地 |
| 16:00 | 返回酒店 | 参赛领队 | 竞赛场地 |
| 竞赛当天 | 07:30 | 裁判就位 | 裁判 | 竞赛场地 |
| 07:30-08:00 | 选手抽签，一次加密 | 参赛选手、裁判 | 竞赛场地 |
| 08:00-08:30 | 选手抽签，二次加密及入场 | 参赛选手、裁判 | 竞赛场地 |
| 08:30-08:50 | 参赛选手就位，宣读考场纪律 | 参赛选手、裁判 | 竞赛场地 |
| 08:50-09:00 | 赛题发放 | 参赛选手、裁判 | 竞赛场地 |
| 09:00-11:00 | 第一阶段比赛时间 | 参赛选手、裁判 | 竞赛场地 |
| 11:00-12:00 | 第二阶段比赛时间 | 参赛选手、裁判 | 竞赛场地 |
| 12:00 | 比赛正式结束 | 参赛选手、裁判 | 竞赛场地 |
| 12:30-评判完毕 | 成绩评判（含晚餐、夜宵） | 裁判长、专家、监督 | 竞赛场地 |
| 竞赛后1日 | 13：30-14：00 | 闭幕式 | 领导、嘉宾、裁判、各参赛队 | 会议室 |

（二）竞赛流程图

**九、竞赛试题**

样题详见附件。

**十、评分标准制定原则、评分方法、评分细则**

（一）评分标准制定原则

根据《全国职业院校技能大赛成绩管理办法》的相关要求，遵循成绩管理基本流程，通过检录、一次加密、二次加密、竞赛成绩评定、解密、成绩公布等流程，规范成绩管理。

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两个阶段的能力和水平。

（二）评分方法

1．参赛队成绩由裁判组统一评定；

2．比赛总分数100分，分为两个阶段单独积分，第一阶段满分为70分，第二阶段满分为30分，每个阶段竞赛系统单独进行自动评分和排名，并在比赛的大屏幕上实时展示；

3．两个阶段采取分步得分、错误不传递、累计总分的积分方式，分别计算环节得分。本赛项为团体赛，由裁判长汇总整理各阶段得分，按参赛队的总成绩进行排名，不计参赛选手个人得分；

4．在竞赛过程中，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，由裁判按照规定扣减相应分数并且给予警告，情节严重的取消竞赛资格，竞赛成绩记0分，队员退出比赛现场；

5．监督组对裁判组的工作进行全程监督，并对竞赛成绩抽检复核。仲裁组负责接受由参赛队领队提出的对裁判结果的申诉，组织复议并及时反馈复议结果；

6．竞赛严格执行裁判遴选管理办法、赛事保密细则和预案、命题管理办法等制度，保证竞赛的公平公正。赞助企业、参赛院校不安排人员进入裁判团队。

（三）评分细则

1.评分阶段：

|  |  |  |  |
| --- | --- | --- | --- |
| **竞赛阶段** | **阶段名称** | **任务阶段** | **评分方式** |
| 第一阶段权重70% | 单兵模式系统渗透测试（本阶段由多个任务组成） | 任务1 | 机考评分 |
| 任务2 | 机考评分 |
| …… | 机考评分 |
| 任务N | 机考评分 |
| 第二阶段权重30% | 分组对抗 | 系统攻防演练 | 机考评分 |

第一阶段分为多个任务，每个任务里面有多个关卡，总分70分。

为保证竞赛的公平公正，所有分数由计算机自动评分，大屏幕直播公开显示。这部分评分需要选手向考评服务器中提交每道题唯一的“KEY”值或者“FLAG”值，系统自动匹配，不需要人工干预。

2.分值比例：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **知识点技能点** | **内容描述** | **分值比例** |
| 1 | 安全防护技术 | HTTP防护、会话跟踪、数据窃取防护、漏洞扫描、防篡改等技术； | 20% |
| 2 | 服务器渗透技术 | 针对未设置防护的数据库和服务器进行扫描、密码猜测等渗透测试； | 30% |
| 3 | 服务器加固技术 | 强制访问控制、数据保护、行为审计等； | 20% |
| 4 | 攻防对抗技术 | 密码学基础、认证与授权基础、Windows/Linux服务器系统与安全、网络服务安全、Web应用安全、数据库安全、扫描探测、溢出攻击、破解验证技术、安全加固、病毒及恶意代码分析及清除等相关知识。 | 30% |

3.整体合分规则

规则1：如果总分相同，以第二阶段评判成绩高低排序，第二阶段评判成绩高者靠前；

规则2：如果第二阶段评判成绩也相同，以第二阶段提交正确FLAG值（实际成绩）高低排序，实际成绩高者排名靠前；

规则3：第二阶段提交正确FLAG值（实际成绩）相同，以第二阶段提交最后一个正确的FALG时间排序，先完成者排名靠前。

4.成绩录入规则

规则1：成绩录入系统的分数不能相同；

规则2：同分选手，按照排名顺序，从最后一位选手开始，排名每靠前一位，增加0.01分录入系统。（或按照排名顺序，从第一位选手开始，排名每靠后一位，减少0.01分录入系统）

竞赛详细评分细则将结合竞赛试题的具体内容由命题组专家设计制定。

**十一、奖项设置**

按照执行《全国职业院校技能大赛奖惩办法》的有关规定。

以赛项实际参赛队数量确定奖项：一等奖占参赛队总数的10%，二等奖占参赛队总数的20%，三等奖占参赛队总数的30%，小数点后四舍五入。

获得一等奖参赛选手的指导教师，由赛项组委会颁发优秀指导教师证书。

**十二、技术规范**

|  |  |  |
| --- | --- | --- |
| **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》 |

**十三、建议使用的比赛器材、技术平台和场地要求**

（一）比赛器材

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **设备型号** |
| 1 | 网络空间安全技能评测平台 | 1 | 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，支持多用户并发在线比赛，根据不同的实战任务下发进行自动调度靶机虚拟化模板，为学员提供单兵闯关、分组混战等实际对战模式，提供超过20种不同级别70个的攻防题目。整个过程全自动评判，自定义动画态势展示，成绩详细分析，多端口监控，全程加密。包含2017年网络空间安全国赛和省赛部分样题和场景。 |
| 2 | PC机 | 2台/赛位 | CPU 主频>=3.5GHZ,>=四核心 八线程；内存>=8G；硬盘>=1T；支持硬件虚拟化；具有串口或者提供USB转串口配置线缆。 |

（二）软件技术平台：

比赛的应用系统环境主要以Windows和Linux系统为主，涉及如下版本：

1）物理机安装操作系统：Windows 7

2）虚拟机安装操作系统：

* Windows系统：Windows XP、Windows 7、Windows2003 Server、Windows2008 Server（根据命题确定）。
* Linux系统：Ubuntu、Debian、CentOS（根据命题确定）。

3）办公软件主要为Microsoft Office 2010(中文版)及以上和RAR 4.0 (中文版)；比赛提供SercureCRT作为终端。

（三）赛场环境要求：

竞赛工位内设有操作平台，每工位配备220V电源，带漏电保护装置，工位内的电缆线应符合安全要求。每个竞赛工位面积6-9㎡，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。

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赛点车辆、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。

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的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。

承办单位应提供保证应急预案实施的条件。对于比赛内容涉及高空作业、可能有坠物、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。

**十四、安全保障**

（一）场地及消防设施：竞赛现场须符合消防安全要求。

（二）线路布置：竞赛现场网线、电源线以及其他线路应符合安全布线要求。

（三）采光与通风：竞赛现场需通风良好、照明需符合教室采光规范。

（四）参赛人员安全：竞赛期间参赛人员（含指导教师和领队）集中住宿、饮食安全。

**十五、经费概算**

竞赛预算主要包括组织预算、场地预算、设备预算三大块。对于上述三项发生的费用，主办方将会协调承办学校、协办企业单位，提供比赛场地、比赛设备（设备使用权）和所需资金。具体方式如下。

1. 组织预算：由承办学校提供；
2. 场地预算：比赛场地由承办学校提供，场地布置费用由承办校和企业共同提供。
3. 设备预算：所用比赛设备由合作企业提供使用权的方式解决。
4. 经费统筹

（1）使用原则：按照“收支平衡、统筹安排、保证重点、专款专用”的使用原则。

（2）使用方向：做好赛事筹备、赛中运营、赛后维护三方面的合理分配与使用。

（3）统筹经费的监督管理：统一监管、具体实施。

1. 经费预算项目清单

|  |  |  |  |
| --- | --- | --- | --- |
| **费用类别** | **项目** | **金额****（万元）** | **备注** |
| 赛项研讨论证、赛题开发及培训预算 | 竞赛方案研讨论证会议组织 | 5 | 研讨会咨询费、差旅费等 |
| 竞赛试题开发 | 5 | 专家封闭开发食宿费、咨询费等 |
| 印刷费 | 2 | 大赛通知、赛程、竞赛文档、赛题等 |
| 培训费 | 1 | 裁判员培训费用 |
| 咨询费 | 3 | 包括命题、评审、裁判等环节 |
| 赛项组织预算 | 场地布置 | 8 | 根据比赛要求布置场地、布线、主席台搭建等 |
| 设备运输、安装、调试 | 6 | 比赛设备运输及安装等 |
| 现场技术支持 | 3 | 竞赛现场支持 |
| 赛项宣传费用 | 5 | 赛场环境设计与制作、宣传材料制作，平面媒体、网站宣传维护等 |
| 服装费 | 4 | 选手、指导老师、裁判、监考、工作人员、志愿服装费 |
| 获奖奖励 | 4 | 获奖人员奖励、奖品和纪念品等 |
| 餐费、交通费 | 6 | 领导、专家、选手在津食、交通费用、工作人员餐费 |
| 赛后资源转化 | 5 | 教材编写、课件制作等专家劳务费用 |
| 预留资金 | 3 | 处理赛事突发事件 |
| 总计 | 60 |  |

**十六、比赛组织与管理**

设立赛项执行委员会，负责整个比赛的组织与管理。

1．设执行委员会主任（总指挥）一名、副主任（副总指挥）二名，负责赛项若干事宜的总体协调。

2．设赛项办公室：组长一名，组员若干，负责支持执行委员会主任、副主任决策的落实与监督。

3．设立仲裁组：组长一名、组员若干，负责赛项的仲裁工作。

4．裁判组：裁判长一名、裁判若干，负责赛项的裁判工作。

5．现场赛务组：组长一名，组员若干，负责赛场场地内设备及人员管理。

6．安保组：组长一名，组员若干，负责赛场及周边的安保工作。

7．秘书组：组长一名，组员若干，负责撰文等文案工作。

8．宣传组：组长一名，组员若干，负责赛项宣传等联系工作。

9．设计组：组长一名，组员若干，负责赛项场地、布展等工作。

10．后勤保障组：组长一名，组员若干，负责住宿、饮食、交通等保障工作。

**十七、教学资源转化建设方案**

（一）2017年赛后资源转化工作

技能大赛的目的是通过大赛活动，深化职业教育教学改革，提高教学质量，为职业学校开放式办学、为高职学生更好的就业、为企业招收到更好的员工提供一个平台， 而大赛的结束却代表着专业建设改革的开始。赛项执委会为了贯彻“以赛促教、以赛促学、以赛促改”的办赛理念，做了如下工作：

1.召开赛项总结会和资源转化会议

为加快全国职业院校技能大赛成果在教学过程中的推广和应用，提升中职学校网络空间安全专业建设水平，提高相关专业学生综合职业能力与素质，赛项执委会于2017年7月14日-15日在江西南昌举办了“2017网络空间安全赛项资源转化会议暨专业建设研讨会”。

会议由2017年全国职业院校技能大赛中职组“网络空间安全”赛项执行委员会主办，南昌市第一中等专业学校、中科软科技股份有限公司协办。会议上由专家组长、裁判长、一等奖获奖学校以及企业做了网络空间安全赛项总结、网络空间安全赛项资源转化方案、网络空间安全赛项备赛训练的经验分享、网络信息安全专业课程建设及实训环境建设的理念与方案、磐云系列产品新功能及学习资源升级计划发布等报告，得到了与会学校的充分认可，对下半年大赛资源转化以及建设“网络与息安全”新专业有了信心和思路。

2.大赛促进师资队伍建设

专业未动、师资先行。信息安全对于中职的学生而言，是有一定难度、较为高端的课程，对于中职的老师而言也是一样，很多学校很早就已经关注到了信息安全产业的发展和人才需求，但就是苦于缺乏师资而不能开设专业。

因此赛项执委会联合赛项合作企业中科软科技，定于2017年7月-8月间在广东江门、江苏常州、湖北武汉、山东青岛等四地举办“网络空间安全”技术专业师资培训班，提升网络空间安全专业师资水平，加快中等职业学校网络空间安全专业建设。

培训不以盈利为目的，向赛项国赛参赛校的指导教师提供了每校一人次的免费参训名额，得到了广大参赛学校的认可。中职计算机教师对于信息安全技术热情高涨，报名积极踊跃，每期培训均超过了原定40人/班的规模。

目前师资培训正在进行中，四期培训结束后，会提供相应的总结报告。

3.大赛促进课程建设

赛项执委会联合专家组和合作企业，在赛后编写了相应授课教材，将赛项转化为教学资源。教材资源是一整套内容：包括课程的专业方向建设、课程内容建设、教学大纲建设、考试大纲建设、认证考试建设、学生职业生涯规划建设等。所有教材依据项目式教学的方法编写，符合先进的职教教学理念。

2017年赛后计划编写3本教材：

《网络信息安全基本理论》：介绍网络安全技术领域的知识体系，在计算机系统领域的知识架构和技术基础，熟悉和掌握计算机系统安全的核心技术，如操作系统安全、网络安全和计算机病毒的防御，掌握关键的安全技术和安全机制、数据的备份与恢复技术、计算机取证技术等，可作为专业技能理论课程。

《系统渗透测试（第一卷）》介绍常用渗透工具的Backtrack 和Kali的使用方法及特定场景下的应用，介绍Python语言基础，了解Python脚本编写，学会利用脚本进行渗透扫描。以实际案例突出其用途和典型配置。

《网络空间安全技能大赛赛题解析》 对2017年该赛项赛题进行解析，分析重、难点及解题步骤与思路，可作为专业技能实训及技能大赛训练使用。

4.网络空间安全赛项教学资源征集活动

为了做好技能大赛资源转化工作，赛项执委会开展了面向全国职业院校征集网络空间安全赛项教学资源的活动。

教学资源分为学习资源和赛题资源，提供了标准的格式要求，针对每一条教学资源需要具备完整的教学资源描述、教学资源场景、教学资源答案和教学资源说明，注明教学资源的作者信息：学校名、作者名、作者电话和邮箱。赛项执委会组织专家对征集的教学资源进行审核、评价。对优秀的教学资源，经作者同意，将作为赛项资源转化成果收入本赛项的赛题库，以备来年省赛、国赛使用，优秀资源的作者将获得适当奖励。

（二）2018年赛后资源转化工作

计划在大赛执委会的领导与监督下，赛后60日内向大赛执委会办公室提交资源转化方案，半年内完成资源转化工作。

1.竞赛过程中获得的主要资源

1. 竞赛样题、试题库；
2. 竞赛技能考核评分案例；
3. 考核环境描述；
4. 竞赛过程音视频记录；
5. 评委、裁判、专家点评；
6. 优秀选手、指导教师访谈。

2.资源转化基本方案与呈现形式

资源转化成果按照行业标准、契合课程标准、突出技能特色、展现竞赛优势，形成满足职业教育教学需求、体现先进教学模式、反映职业教育先进水平的共享性职业教育教学资源。资源转化成果包含基本资源和拓展资源，充分体现本赛项技能考核特点：

1. 基本资源：

基本资源按照技能概要、训练单元、训练资源三大模块设置：

* 技能概要包括技能介绍、训练大纲、技能要点、评价指标等。
* 训练单元按任务模块或技能模块组织设置，可包括演示文稿、操作流程演示视频/动画等。
* 训练资源可包括教学方案、训练指导、作业/任务、实验/实训/实习资源等。训练资源模块可单独列出，也可融入各训练单元。
1. 拓展资源：

拓展资源以反映技能特色为主，应用于各教学与训练环节，支持技能教学和学习过程，较为成熟的多样性辅助资源。例如：点评视频、访谈视频、试题库、案例库、素材资源库等。

3.资源的技术标准

资源转化成果以文本文档、演示文稿、视频文件、Flash文件、图形/图像素材和网页型资源等，技术标准符合《全国职业院校技能大赛资源转化工作办法》的要求。

4.资源的提交方式与版权

赛项资源转化成果的版权由技能大赛执委会和赛项执委会共享。

5.资源的使用与管理

资源转化成果的使用与管理由大赛执委会统一使用与管理，会同赛项承办单位、赛项有关专家，联系出版社编辑出版有关赛项试题库、岗位典型操作流程等精品资源。

6.资源转化项的工作进程表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **一级资源项** | **二级资源项** | **内容简述** | **转化方式** | **进度安排** | **备注** |
| 风采展示 | 赛项宣传片 | 介绍大赛主题、目的、意义以及实施过程，突出展现参赛选手同台竞技的风采。 | 15分钟视频 | 赛后5天内完成 | 1.承办校比赛当天全程摄像，拍摄比赛各个阶段2. 承办校拍摄教师休息区和大屏展示区采集素材 |
| 获奖选手风采展示片 | 介绍选手日常学习、备赛、参赛、获奖等环节的感受。 | 10分钟视频 | 赛后5天内完成 | 1. 承办校闭幕式之后，访谈拍摄大赛一等奖参赛队2.赛项执委会通知各个参赛队留存日常训练视频，比赛当天提供给承办校用于剪辑 |
| 技能概要 | 技能介绍 | 介绍大赛相关技能 | 编写相关文本资料 | 赛后60天内完成 | 赛项专家组完成 |
| 训练大纲 | 介绍大赛训练过程要点 | 编写相关文本资料 | 赛后60天内完成 | 赛项专家组完成 |
| 评价指标 | 介绍大赛评价指标 | 编写相关文本资料 | 赛后60天内完成 | 赛项专家组完成 |
| 教学资源 | 网络空间安全进阶-渗透测试第二卷 | 该门课程可作为中职网络信息安全专业的专业核心课，适合学有余力的本专业学生进一步加深学习 | 教材、文档、图片、视频、仿真课件等 | 赛后60天内完成 | 包括教学方案、训练指导、作业/任务、实验/实训/实习资源等。教学单元按任务模块或技能模块组织设置， 包括演示文稿、图片、操作流程演示视频、提供交互式仿真实训课件。 |
| 网络空间安全大赛项目解析2018 | 对2018年该赛项赛题进行解析，分析重点、难点。可供中职学校网络信息安全专业师生进行综合项目实训以及技能大赛训练使用 | 教材、文档、图片、视频、仿真课件等 | 赛后60天内完成 | 包括教学方案、训练指导、作业/任务、实验/实训/实习资源等。教学单元按任务模块或技能模块组织设置， 包括演示文稿、图片、操作流程演示视频、提供交互式仿真实训课件。 |

**十八、筹备工作进度时间表**

|  |  |  |
| --- | --- | --- |
| **序号** | **时间** | **事项** |
| 1 | 2017年8月 | 组建赛项申报专家组，编写申报材料 |
| 2 | 2017年10月-12月 | 赛项初次答辩，组织专家组对方案进行细节讨论和调整 |
| 3 | 2017年12月 | 赛事技术文件网上预发布确定比赛场地 |
| 4 | 2018年1月 | 场地布置规划召开专家组会议，并提交正式公布的竞赛规程成立技术组，召开技术组会议研究与竞赛有关的细节问题并分工准备、大赛样题（或试题）设计 |
| 5 | 2018年3月初 | 讨论国赛试题参赛队报名 |
| 6 | 2018年3月中 | 公布竞赛样题（或试题）和评分标准设备安装、测试（少量）裁判申报 |
| 7 | 2018年3月底 | 参赛队报名截止确定裁判比赛场地基础条件布置完毕 |
| 8 | 2018年4月初 | 所有赛项文件汇总报秘书处 |
| 9 | 2018年4月10日 | 确定命题人选设备、器材、用品全部到位 |
| 10 | 2018年4月15日 | 现场启动 |
| 11 | 2018年4月15-22日 | 考题确定比赛设备安装与调试 |
| 12 | 2018年4月23日 | 启动正式比赛流程 |
| 13 | 2018年6月底 | 赛项成果汇总材料报相关单位 |

**十九、裁判人员建议**

裁判人员整体要求如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **专业技术方向** | **知识能力要求** | **执裁、教学、工作经历** | **专业技术职称****（职业资格等级）** | **人数** |
| 1 | 信息安全、网络安全、计算机网络、计算机应用方向 | 熟悉网络基础以及windows和Linux操作系统，熟悉网络安全类别和主要攻防手段 | 具有信息安全教学和国赛执裁经验 | 高级 | 10 |
| 2 | 信息技术类 | 熟悉网络基础以及windows | 具有省级赛事执裁经验 | 副高 | 10 |
| **裁判总人数** | 20 |

赛项所需裁判工作岗位分类需求如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **裁判类别** | **从事专业** | **知识能力要求** | **职称** | **数量** |
| 裁判长 | 信息安全、网络安全、计算机网络、计算机应用方向 | 熟悉网络基础以及windows和Linux操作系统，熟悉网络安全类别和主要攻防手段 | 高级 | 1 |
| 现场裁判 | 信息安全、网络安全、计算机网络、计算机应用方向 | 熟悉网络基础以及windows和Linux操作系统，熟悉网络安全类别和主要攻防手段 | 副高及以上 | 14 |
| 加密裁判 | 信息技术类 | 熟悉网络基础以及windows | 中级以上 | 3 |
| 统分裁判 | 信息技术类 | 熟悉网络基础以及windows | 中级以上 | 2 |
| 合计 | 20人 |

**二十、其他**

承诺赛题全部公开。本赛项将于开赛 1 个月前，在大赛网络信息发布平台上（www.chinaskills-jsw.org）公开赛题。

同期举办包括针对学生、带队教师的活动、校企合作论坛、新技术展示、媒体宣传等。

**附件：**

**中职组“网络空间安全”赛项样题**

一、竞赛阶段简介

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **任务阶段** | **竞赛任务** | **竞赛时间** | **分值** |
| 第一阶段单兵模式系统渗透测试 | 任务1 | Linux操作系统服务渗透测试及安全加固 | 两小时 | 25 |
| 任务2 | Windows操作系统服务渗透测试及安全加固 | 25 |
| 任务3 | Windows操作系统服务端口扫描渗透测试 | 20 |
| 第二阶段分组对抗 | 系统加固 | 一小时 | 30 |
| 渗透测试 |

二、拓扑图



三、竞赛任务书

（一）第一阶段任务书（70分）

根据《赛场参数表》提供的信息，请使用PC1的谷歌浏览器登录考试平台，登录后点击“闯关关卡”，左侧有本阶段的三个任务列表。

点击右侧的“网络靶机”，进入虚机完成任务，找到FLAG值，填入空框内，点击“提交任务”按钮。

提示： FLAG中包含的字符是英文字符，注意英文字符大小写区分。

虚拟机1：Ubuntu Linux 32bit（用户名：root；密码：toor）；

虚拟机1安装工具集：Backtrack5；

虚拟机1安装开发环境：Python；

虚拟机2：WindowsXP（用户名：administrator；密码：123456）。

任务1. Linux操作系统服务渗透测试及安全加固（25分）

**任务环境说明：**

* 服务器场景：CentOS5.5（用户名：root；密码：123456）
* 服务器场景操作系统：CentOS5.5
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：FTP
* 服务器场景操作系统安装服务：SSH
* 服务器场景操作系统安装开发环境：GCC
* 服务器场景操作系统安装开发环境：Python

1.在服务器场景CentOS5.5上通过Linux命令行开启HTTP服务，并将开启该服务命令字符串作为FLAG值提交；（3分）

2.通过PC2中渗透测试平台对服务器场景CentOS5.5进行操作系统扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作使用命令中必须要使用的参数作为FLAG提交；（3分）

3.通过PC2中渗透测试平台对服务器场景CentOS5.5进行操作系统扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作显示结果“OS Details：”之后的字符串作为FLAG提交；（3分）

4.通过PC2中渗透测试平台对服务器场景CentOS5.5进行系统服务及版本号扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作使用命令中必须要使用的参数作为FLAG提交；（4分）

5.通过PC2中渗透测试平台对服务器场景CentOS5.5进行系统服务及版本号扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作显示结果的HTTP服务版本信息字符串作为FLAG提交；（4分）

6.在服务器场景CentOS5.5上通过Linux命令行关闭HTTP服务，并将关闭该服务命令字符串作为FLAG值提交；（4分）

7.再次通过PC2中渗透测试平台对服务器场景CentOS5.5进行系统服务及版本号扫描渗透测试（使用工具NMAP，使用必须要使用的参数），并将该操作显示结果的第2项服务的PORT信息字符串作为FLAG提交。（4分）

任务2. Windows操作系统服务渗透测试及安全加固（25分）

**任务环境说明：**

* 服务器场景：WinServ2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Microsoft Windows2003 Server
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：CA
* 服务器场景操作系统安装服务：SQL

1.PC2虚拟机操作系统WindowsXP打开Ethereal，验证监听到PC2虚拟机操作系统WindowsXP通过Internet Explorer访问IISServ2003服务器场景的Test.html页面内容，并将Ethereal监听到的Test.html页面内容在Ethereal程序当中的显示结果倒数第2行内容作为FLAG值提交；（7分）

2.在PC2虚拟机操作系统WindowsXP和WinServ2003服务器场景之间建立SSL VPN，须通过CA服务颁发证书；IISServ2003服务器的域名为www.test.com，并将WinServ2003服务器个人证书信息中的“颁发给：”内容作为FLAG值提交；（8分）

3.在PC2虚拟机操作系统WindowsXP和WinServ2003服务器场景之间建立SSL VPN，再次打开Ethereal，监听Internet Explorer访问WinServ2003服务器场景流量，验证此时Ethereal无法明文监听到Internet Explorer访问WinServ2003服务器场景的HTTP流量，并将WinServ2003服务器场景通过SSL Record Layer对Internet Explorer请求响应的加密应用层数据长度（Length）值作为FLAG值提交。（10分）

任务3. Windows操作系统服务端口扫描渗透测试（20分）

**任务环境说明：**

* 服务器场景：WinServ2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Microsoft Windows2003 Server
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：CA
* 服务器场景操作系统安装服务：SQL

1.进入PC2虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG1字符串，将该字符串作为FLAG值（形式：FLAG1字符串）提交； （2分）

2.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG2字符串，将该字符串作为FLAG值（形式：FLAG2字符串）提交； （2分）

3.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG3字符串，将该字符串作为FLAG值（形式：FLAG3字符串）提交； （2分）

4.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG4字符串，将该字符串作为FLAG值（形式：FLAG4字符串）提交； （2分）

5.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG5字符串，将该字符串作为FLAG值（形式：FLAG5字符串）提交；（3分）

6.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG6字符串，将该字符串作为FLAG值（形式：FLAG6字符串）提交；（3分）

7.进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，填写该文件当中空缺的FLAG7字符串，将该字符串作为FLAG值（形式：FLAG7字符串）提交；（3分）

8.在虚拟机操作系统：Ubuntu Linux 32bit下执行tcpportscan.py文件，对目标HTTP服务器应用程序工作传输协议、端口号进行扫描判断，将该文件执行后的显示结果中，包含TCP 80端口行的全部字符作为FLAG值提交。（3分）

（二）第二阶段任务书（30分）

假定各位选手是某电子商务企业的信息安全工程师，负责企业某服务器的安全防护，该服务器可能存在着各种问题和漏洞。你需要尽快对该服务器进行安全加固，15分钟之后将会有其它参赛队选手对这台服务器进行渗透。

根据《赛场参数表》提供的第二阶段的信息，请使用PC1的谷歌浏览器登录考试平台。

提示1：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

提示2：加固全部漏洞；

提示3：对其它参赛队服务器进行渗透，取得FLAG值并提交到自动评分系统；

提示4：十五分钟之后，各位选手才可以进入渗透测试环节。渗透测试环节中，各位选手可以继续加固服务器，也可以选择攻击其他选手的服务器。

**靶机环境说明：**

* 服务器场景：CentOS5.5（用户名：root；密码：123456）
* 服务器场景操作系统：CentOS5.5
* 服务器场景操作系统安装服务：HTTP
* 服务器场景操作系统安装服务：FTP
* 服务器场景操作系统安装服务：SSH
* 服务器场景操作系统安装服务：SQL
* 服务器场景操作系统安装开发环境：GCC
* 服务器场景操作系统安装开发环境：Python
* 服务器场景操作系统安装开发环境：PHP

**可能的漏洞列表如下：**

1.靶机上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限;

2.靶机上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限;

3.靶机上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权;

4.操作系统提供的服务可能包含了远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限;

5.操作系统提供的服务可能包含了缓冲区溢出漏洞，要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限;

6.操作系统中可能存在一些系统后门，选手可以找到此后门，并利用预留的后门直接获取到系统权限。

**注意事项：**

注意1：任何时候不能人为关闭服务器服务端口，否则将判令停止比赛，第二阶段分数为0分；

注意2：不能对裁判服务器进行攻击，否则将判令停止比赛，第二阶段分数为0分；

注意3：在加固阶段（前十五分钟，具体听现场裁判指令）不得对任何服务器进行攻击，否则将判令攻击者停止比赛，第二阶段分数为0分；

注意4：FLAG值为每台受保护服务器的唯一性标识，每台受保护服务器仅有1个；

注意5：靶机的FLAG值存放在./root/Flaginfoxxxx.xxx.txt文件内容当中（xxxx.xxx是随机产生的字符）；

注意6：在登录自动评分系统后，提交对手靶机的FLAG值，同时需要指定对手靶机的IP地址；

注意7：不得人为恶意破坏自己服务器的FLAG值，一经发现将判令犯规，第三阶段分数为0分；

注意8：本环节是对抗环节，不予补时。

**第二阶段评分说明：**

规则1：每提交1次对手靶机的FLAG值增加2分，每当被对手提交1次自身靶机的FLAG值扣除2分，每个对手靶机的FLAG值只能提交一次；

规则2：第二阶段总分为30分，初始分为10分。在实际得分和大屏显示中，某选手得分可能会显示负分或者超过30分；凡是负分的，本阶段评判成绩一律为0分；凡是超过30分的，本阶段评判成绩一律为30分。

（样题完）