**2017年全国职业院校技能大赛中职组**

**“网络空间安全”赛项规程**

# 一、赛项名称

赛项编号：ZZ-2017024

赛项名称：网络空间安全

英语翻译：[Cyberspace Security](http://www.baidu.com/link?url=Ltb-4t1FNAs7ZPE6xtBnVYCgbAb-538XHRCKjaCuJRg5urKbS0R2HQWwtRjzqW6_5TWgxixiDaVIqbwDE2E0OHejjwXEgTCBXWAi_qxQguuYy2FVw5RNy3Pcanpmcg-_)

赛项组别：中职

赛项归属产业：电子信息产业

# 二、竞赛目的

通过竞赛，检验参赛选手对网络、服务器系统等网络空间中各个信息系统的安全防护能力，以及分析、处理现场问题的能力。通过本赛项的训练和比赛，培养更多学生掌握网络安全知识与技能，发展成为国家信息安全领域的技术技能人才。引导中等职业学校关注网络安全技术发展趋势和产业应用方向，促进网络信息安全专业建设与教学改革。赛项紧密结合新一代信息产业发展对网络安全应用型人才的需求，促进产教互动、校企融合，增强中职学校学生的新技术学习能力和就业竞争力，助力新一代信息技术产业快速发展。

# 三、竞赛内容

重点考核参赛选手网络连通、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业务需求和实际的工程应用环境，实现网络设备、终端设备、服务器的连接，通过调试，实现网络互联互通。

2.参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，以满足应用需求。

3.参赛选手能够根据大赛提供的赛项要求，设计网络空间安全防护方案，并且能够提供详细的网络空间安全防护设备部署拓扑图。

4.参赛选手能够根据网络实际运行中面临的安全威胁，确定安全策略并部署实施，防范并制止网络恶意入侵和攻击行为。

5.进行分组混合对抗，在防护选手自己服务器的同时，渗透其他任意对手的服务器，比赛结果通过大屏幕等形式实时展示。

6.竞赛总时长为3个小时，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 | 单兵模式系统渗透测试 | 访问控制 | 保护内网服务安全，实现防DOS、DDOS攻击、包过滤、应用层代理等； |
| 密码学和VPN | 密码学基础、IPSec VPN、IKE：PreShared Key（预共享密钥认证）、IKE：PKI（公钥架构认证）、SSL VPN等； |
| 操作系统渗透测试及加固 | Windows操作系统渗透测试及加固、Linux操作系统渗透测试及加固等； |
| Web应用渗透测试及加固 | SQL Injection（SQL注入）漏洞渗透测试及加固、Command Injection（命令注入）漏洞渗透测试及加固、File Upload（文件上传）漏洞渗透测试及加固、Directory Traversing（目录穿越）漏洞渗透测试及加固、XSS（Cross Site Script）漏洞渗透测试及加固、CSRF（Cross Site Request Forgeries）漏洞渗透测试及加固、Session Hijacking（会话劫持）漏洞渗透测试及加固 |
| 网络安全数据分析 | 能够利用日志系统和协议分析等系统对网络内的数据进行分析，把控网络安全等； |
| 第二阶段 | 攻防对抗 | 参赛选手之间进行对抗演练 | Windows/Linux操作系统安全攻防、Web应用/数据库安全攻防等； |

7.竞赛分值权重和时间安排

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容模块** | **分值权重** | **竞赛时间** |
| 第一阶段 | 单兵模式系统渗透测试 | 70% | 120分钟 |
| 第二阶段 | 攻防对抗 | 30% | 60分钟 |

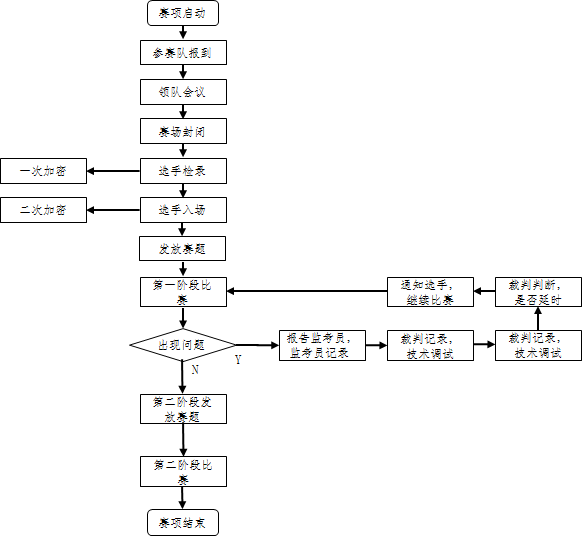
# 四、竞赛方式

1.本赛项为个人赛。

2.同一学校报名人数不超过2人。

3.每名选手限报1名指导教师，指导教师须为本校专兼职教师。

# 五、竞赛流程

（一）竞赛流程图

（二）竞赛时间表

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、专家组 | 会议室 |

# 六、竞赛试题

（一）赛项执委会专家组下设的命题组负责本赛项命题工作。

（二）本赛项为公开赛题，竞赛真题距国赛开始日1月之前公开。

（三）本赛项通过全国职业院校技能大赛指定的网络信息发布平台（http://www.chinaskills-jsw.org）公布竞赛真题。

样题见附件。

# 七、竞赛规则

（一）报名资格

参赛选手须为2017年度在籍全日制中等职业学校学生；五年制全日制高职一至三年级（含三年级）在籍学生可参加比赛。参赛选手不限性别，年龄须不超过21周岁，年龄计算的截止时间以2017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。

（四）参赛选手自行决定工作程序和时间安排。

（五）参赛选手在赛前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，参赛选手要确认已成功提交所有竞赛文档，裁判员与参赛选手一起签字确认，参赛选手在确认后不得再进行任何操作。

# 八、竞赛环境

1.竞赛场地。竞赛现场设置竞赛区、裁判区、服务区、技术支持区。现场保证良好的采光、照明和通风；提供稳定的水、电和供电应急设备。同时提供所有指导教师休息室1间。

2.竞赛设备。竞赛设备由执委会和承办校负责提供和保障，竞赛区按照参赛队数量准备比赛所需的软硬件平台，为参赛队提供标准竞赛设备。

3.竞赛工位。竞赛现场各个工作区配备单相220V/3A以上交流电源。每个比赛工位上标明编号。每个比赛间配有工作台，用于摆放计算机和其它调试设备工具等。配备2把工作椅（凳）。

4.技术支持区为参赛选手比赛提供网络环境部署和网络安全防范。

5.服务区提供医疗等服务保障。

6.竞赛工位隔离和抗干扰。竞赛工位之间标有隔离线，每个相邻竞赛赛位隔离线之间间隔不低于1.5米。

# 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，参赛选手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）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 | 中科软磐云PY-B7  磐云PY-B7为1U设备，2个千兆以太口， Intel至强处理器，16G内存，120G SSD +1T SATA硬盘。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功能,为学员提供单兵闯关、分组混战和夺旗竞速等实际对战模式，能够提供29种不同级别的攻防场景。 |
| 2 | PC机 | 2 | 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。

# 十一、成绩评定

（一）裁判工作原则

按照《2016年全国职业院校技能大赛专家和裁判工作管理办法》建立全国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，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。

本赛项拟设裁判14名。分为裁判长、加密裁判、现场裁判。

因为本赛项全部分数由计算机自动评分，因此只需进行两次加密，加密后参赛选手中途不得擅自离开赛场。分别由2组加密裁判组织实施加密工作，管理加密结果。监督员全程监督加密过程。

第一组加密裁判，组织参赛选手进行第一次抽签，产生参赛编号，替换选手参赛证等个人身份信息，填写一次加密记录表连同选手参赛证等个人身份信息证件，装入一次加密结果密封袋中单独保管。

第二组加密裁判，组织参赛选手进行第二次抽签，确定赛位号，替换选手参赛编号，填写二次加密记录表连同选手参赛编号，装入二次加密结果密封袋中单独保管。

所有加密结果密封袋的封条均需相应加密裁判和监督人员签字。密封袋在监督人员监督下由加密裁判放置于保密室的保险柜中保存。

（二）裁判评分方法

裁判组监督现场机考评分，由裁判长负责竞赛全过程。

竞赛现场派驻监督员、裁判员、监考员、技术支持队伍等，分工明确。根据现场环境，每位监考员负责10名参赛选手，5-6名技术支持工程师负责所有工位设备应急。监考员负责与参赛选手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

计算机自动评分，由裁判长负责将竞赛两个阶段的分数汇总，产生每赛位号的对应成绩。

裁判长在竞赛结束18小时内正式提交赛位号对应的评分结果并复核无误后，加密裁判在监督人员监督下对加密结果进行逐层解密，形成成绩一览表，成绩表由裁判长、监督员签字确认后公布。

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** | **阶段名称** | **任务阶段** | **竞赛任务** | **分值** | **评分方式** |
| 第一阶段  权重70% | 单兵模式系统渗透测试 | 任务1 | 根据赛题确定内容 | 25 | 机考评分 |
| 任务2 | 根据赛题确定内容 | 25 | 机考评分 |
| 任务2 | 根据赛题确定内容 | 20 | 机考评分 |
| 第二阶段  权重30% | 分组对抗 | 系统攻防 | | 30 | 机考评分 |

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。

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。

# 十二、奖项设定

本赛项为个人赛，依照实际参赛选手数量确定奖项：一等奖占参赛选手总数的10%，二等奖占参赛选手总数的20%，三等奖占参赛选手总数的30%。

获得一等奖的参赛队指导教师获“优秀指导教师奖”，授予荣誉证书。

# 十三、赛项安全

赛事安全是全国职业院校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。

1. 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，建立公安、消防、司法行政、交通、卫生、食品、质检等相关部门协调机制保证比赛安全。制定相应安全管理的规范、流程和突发事件应急预案，及时处置突发事件，全过程保证比赛筹备和实施工作安全。

1. 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。

1. 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；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，确认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。

整个大赛过程邀请当地公安系统、卫生系统和保险系统协助支持。

参赛选手旅途及竞赛过程中的安全保障由各省市负责。

4. 赛项执委会须在赛前组织专人对比赛现场、住宿场所和交通保障进行考察，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。承办单位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。

6. 承办单位应提供保证应急预案实施的条件。对于内容涉及高空作业、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。

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、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。

1. 生活条件

1. 比赛期间，原则上由赛事承办单位统一安排参赛选手和指导教师食宿。承办单位须尊重少数民族的信仰及文化，根据国家相关的民族政策，安排好少数民族选手和教师的饮食起居。

2. 比赛期间安排的住宿地应具有宾馆/住宿经营许可资质。以学校宿舍作为住宿地的，大赛期间的住宿、卫生、饮食安全等由赛项执委会和提供宿舍的学校共同负责。

3. 大赛期间组织的参观和观摩活动，由赛区组委会负责。赛项执委会和承办单位须保证比赛期间选手、指导教师和裁判员、工作人员的交通安全。

4. 各赛项的安全管理，除了采取必要的安全隔离措施外，应严格遵守国家相关法律法规，保护个人隐私和人身自由。

1. 组队责任

1. 各省、自治区、直辖市和计划单列市在组织参赛时，须安排为参赛选手购买大赛期间的人身意外伤害保险。

2. 各省、自治区、直辖市和计划单列市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。

3. 各参赛选手领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。

1. 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。

1. 处罚措施

1. 赛项出现重大安全事故的，停止承办单位的赛项承办资格。

2. 因参赛选手原因造成重大安全事故的，取消其参赛资格。

3. 参赛选手有发生重大安全事故隐患，经赛场工作人员提示、警告无效的，可取消其继续比赛的资格。

4. 赛事工作人员违规的，按照相应的制度追究责任。情节恶劣并造成重大安全事故的，由司法机关追究相应法律责任。

# 十四、竞赛须知

（一）参赛选手须知

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。

（二）指导教师须知

1.各参赛代表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.各代表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。

4.参赛代表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，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或对处理意见不服而停止竞赛，否则以弃权处理。

6.指导老师应及时查看大赛专用网页有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、技术规范和赛场要求，指导选手做好赛前的一切技术准备和竞赛准备。

7. 参赛选手领队应对本队参赛选手和指导教师的参赛期间安全负责，参赛学校须为参赛选手和指导教师购买意外保险。

8. 领队和指导教师应在赛后做好赛事总结和工作总结。

（三）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，按照各自职责分工和要求认真做好岗位工作。

2. 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。

# 十五、申诉与仲裁

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

书面申诉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，并由领队亲笔签名。非书面申诉不予受理。

赛项仲裁工作组在接到申诉报告后的2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。申诉方对复议结果仍有异议，可由省（市）领队向赛区仲裁委员会提出申诉。赛区仲裁委员会的仲裁结果为最终结果。

# 十六、竞赛观摩

本赛项将会设计观摩区，使用大屏幕实时显示第二阶段和第三阶段网络空间攻防及对战的进度。

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。

# 十七、竞赛直播

赛项全程录像。

本赛项赛前对赛题保密、设备安装调试、软件安装等关键环节进行实况摄录。竞赛过程采用全程摄录的形式，对比赛的开闭幕式、比赛过程、手工评卷等过程进行全程实况转播。

本赛况在赛后将制作大赛制作优秀选手采访、优秀指导教师采访、裁判专家点评和企业人士采访视频资料。

# 十八、资源转化

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。

（一）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。

（二）资源转化基本方案与呈现形式

资源转化成果遵循行业标准,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：

（1）技能概要包括技能介绍、训练大纲、技能要点、评价指标等。

（2）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。

（3）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。

2.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。

（三）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：

1.文本文档：采用DOC或DOCX格式。文件制作所使用的软件版本不低于Microsoft Office 2003。

2.演示文稿：采用PPT或PPTX格式。文件制作所使用的软件版本不低于Microsoft Office 2003。尽可能少用宏，播放时不要出现宏脚本提示。

3.视频文件：采用MP4格式。录像环境光线充足、安静，衣着得体，语音清晰。

（1）视频压缩采用H.264(MPEG-4 Part10：profile=main, level=3.0)编码方式，码流率256 Kbps以上，帧率不低于25 fps，分辨率不低于720×576（4:3）或1024×576（16:9）。

（2）声音和画面要求同步，无交流声或其他杂音等缺陷，无明显失真、放音过冲、过弱。伴音清晰、饱满、圆润，无失真、噪声杂音干扰、音量忽大忽小现象。解说声与现场声、背景音乐无明显比例失调。音频信噪比不低于48 dB。

（3）字幕要使用符合国家标准的规范字，不出现繁体字、异体字(国家规定的除外)、错别字；字幕的字体、大小、色彩搭配、摆放位置、停留时间、出入屏方式力求与其他要素（画面、解说词、音乐）配合适当，不能破坏原有画面。

（4）Flash文件：文件制作所使用的软件版本不低于Flash 6.0。

（5）图形/图像素材：采用常见存储格式，如GIF、PNG、JPG等。彩色图像颜色数不低于真彩（24位色），灰度图像的灰度级不低于256级，屏幕分辨率不低于1024×768时，扫描图像的扫描分辨率不低于72 dpi。

（6）网页型资源：交互式仿真实训资源。兼容Microsoft IE、Google Chrome、Mozilla Firefox浏览器。避免出现大量的垃圾代码，使用网页编辑工具编辑网页，不可直接将Microsoft Word、WPS等文件内容粘贴到网页文件中。

（四）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。

（五）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。

（六）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9号闭幕式之后，访谈拍摄大赛一等奖参赛选手  2.赛项执委会通知各个参赛选手留存日常训练视频，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 | 网络空间安全基础 | 该门课程可作为中职网络与安全专业的基础入门课程，适合本专业全体学生学习 | 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。 |
| 网络空间安全进阶 | 该门课程可作为中职信息安全的进阶课程，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 | 对2017年该赛项赛题进行解析，分析重点、难点。可供中职信息安全专业学校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。 |

# 附件：样题

**“网络空间安全”项目竞赛任务书（样题）**

**一、赛项时间**

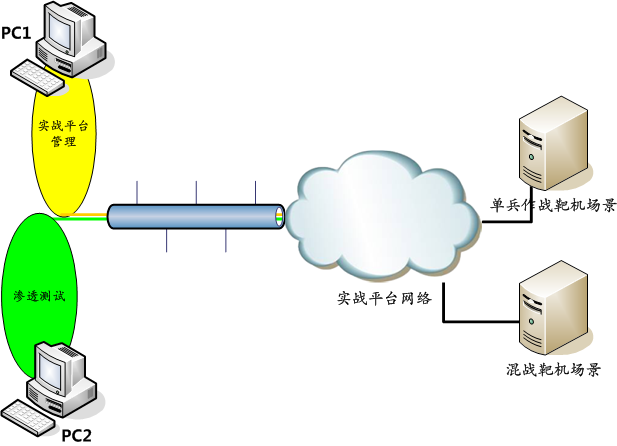
9:00-12:00，共计3小时。

**二、赛项信息**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | SQL注入攻防 | 09:00-11:00 | 25 |
| 任务2 | XSS和CSRF攻防 | 25 |
| 任务3 | 命令注入与文件包含攻防 | 20 |
| 第二阶段  分组对抗 | 系统攻防 | | 11:00-12:00 | 30 |

**（一）赛项环境设置**

**1.网络拓扑图**



**2.IP地址规划表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **接口** | **IP地址** | **互联** | **可用IP数量** |
| PC-1：实战平台管理机 | EthX | x.x.x.x/x | 与实战平台管理网络相连 | 见赛场IP参数表 |
| PC-2：渗透测试机 | EthY | x.x.x.x/x | 与渗透测试网络相连 | 见赛场IP参数表 |
| 服务器场景 | 无 | 详见赛题部分 | | 见赛场IP参数表 |
| 备注 | 1.赛题可用IP地址范围见《赛场IP参数表》；  2.具体网络连接接口见《赛场IP参数表》-“赛场互联接口参数表”；  3.设备互联网段内可用地址数量见《赛场IP参数表》；  4.IP地址分配要求，最节省IP地址，子网有效地址规划遵循2n-2的原则；  5.参赛选手按照《赛场IP参数表》要求，自行分配IP地址段、设备互联接口；  6.将分配的IP地址段和接口填入《赛场IP参数表》中（《赛场IP参数表》电子文件存于U盘“第一阶段”文件夹中，请填写完整后提交。） | | | |

**（二）第一阶段任务书（70分）**

任务1：SQL注入攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具1：Apache2.2；

服务器场景安装服务/工具2：Php6；

服务器场景安装服务/工具3：Microsoft SqlServer2000；

服务器场景安装服务/工具4：EditPlus；

1. 访问WebServ2003服务器场景，进入login.php页面，分析该页面源程序，找到提交的变量名，并将该变量名作为Flag提交；

2. 对该任务题目1页面注入点进行SQL注入渗透测试，使该Web站点可通过任意用户名登录，并将登录密码作为Flag提交；

3. 进入WebServ2003服务器场景的C:\AppServ\www目录，找到loginAuth.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御SQL注入，并将修改后的PHP源程序中的Flag提交；

4. 再次对该任务题目1页面注入点进行渗透测试，验证此次利用该注入点对WebServ2003服务器场景进行SQL注入渗透测试无效，并将Web页面回显内容作为Flag提交；

5. 访问WebServ2003服务器场景，"/"->"Employee Information Query"，分析该页面源程序，找到提交的变量名，并将该变量名作为Flag提交；

6. 对该任务题目5页面注入点进行渗透测试，根据输入“%”以及“\_”的返回结果确定是注入点，Web页面回显作为Flag提交；

7. 通过对该任务题目5页面注入点进行SQL注入渗透测试，删除WebServ2003服务器场景的C:\目录下的1.txt文档，并将注入代码作为Flag提交；

8. 进入WebServ2003服务器场景的C:\AppServ\www目录，找到QueryCtrl.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御SQL注入渗透测试，并将修改后的PHP源程序中的Flag提交；

9. 再次对该任务题目5页面注入点进行渗透测试，验证此次利用注入点对该WebServ2003服务器场景进行SQL注入渗透测试无效，并将Web页面回显内容作为Flag提交。

任务2：XSS和CSRF攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具1：Apache2.2；

服务器场景安装服务/工具2：Php6；

服务器场景安装服务/工具3：Microsoft SqlServer2000；

服务器场景安装服务/工具4：EditPlus；

1. 访问WebServ2003服务器场景，"/"->" Employee Message Board"，分析该页面源程序，找到提交的变量名，并将该变量名作为Flag提交；

2. 对该任务题目1页面注入点进行XSS渗透测试，并进入"/"->" Employee Message Board"->"Display Message"页面，根据该页面的显示，确定是注入点，并将Web页面回显内容作为Flag提交；

3. 对该任务题目1页面注入点进行渗透测试，使"/"->" Employee Message Board"->"Display Message"页面的访问者执行网站（http://hacker.org/）中的木马程序：http://hacker.org/TrojanHorse.exe，并将注入代码内容作为Flag提交；

4. 通过IIS搭建网站（http://hacker.org/），并通过PC2生成木马程序TrojanHorse.exe，将该程序复制到网站（http://hacker.org/）的WWW根目录下，并将该网站标题作为Flag提交；

5. 当"/"->" Employee Message Board"->"Display Message"页面的访问者执行网站（http://hacker.org/）中的木马程序TrojanHorse.exe以后，访问者主机需要被PC-3远程控制，打开访问者主机的CMD.exe命令行窗口，并将该操作结果回显作为Flag提交；

6. 进入WebServ2003服务器场景的C:\AppServ\www目录，找到insert.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御XSS渗透测试，并将修改后的PHP源程序中的Flag提交；

7. 再次对该任务题目1页面注入点进行渗透测试，验证此次利用该注入点对WebServ2003服务器场景进行XSS渗透测试无效，并将Web页面回显作为Flag提交；

8. 访问WebServ2003服务器场景，"/"->" Shopping Hall"，分析该页面源程序，找到提交的变量名，并将该变量名作为Flag提交；

9. 对该任务题目1页面注入点进行渗透测试，使"/"->" Employee Message Board"->"Display Message"页面的访问者向页面ShoppingProcess.php提交参数goods=cpu&quantity=999999，查看"/"->"PurchasedGoods.php页面，并将注入代码作为Flag提交；

10. 进入WebServ2003服务器场景的C:\AppServ\www目录，找到DisplayMessage.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御CSRF渗透测试，并将修改后的源程序中的Flag提交；

11. 再次对该任务题目1页面注入点进行渗透测试，验证此次利用该注入点对WebServ2003服务器场景进行CSRF渗透测试无效，并将Web页面回显内容作为Flag提交；

任务3：命令注入与文件包含攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具1：Apache2.2；

服务器场景安装服务/工具2：Php6；

服务器场景安装服务/工具3：Microsoft SqlServer2000；

服务器场景安装服务/工具4：EditPlus；

1. Web访问WebServ2003服务器场景，"/"->" Display Directory"，分析该页面源程序，找到提交的变量名，并将该变量名作为Flag提交；

2. 对该任务题目1页面注入点进行渗透测试，使页面DisplayDirectoryCtrl.php回显C:\Windows目录内容的同时，对WebServ2003服务器场景添加账号“Hacker”，将该账号加入管理员组，并将注入代码作为Flag提交；

3. 进入WebServ2003服务器场景的C:\AppServ\www目录，找到DisplayDirectoryCtrl.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御命令注入渗透测试，并将修改后的源程序中的Flag提交；

4. 再次对该任务题目1页面注入点进行渗透测试，验证此次利用注入点对WebServ2003服务器场景进行命令注入渗透测试无效，并将Web页面回显作为Flag提交；

5. Web访问WebServ2003服务器场景，"/"->" Display Uploaded's File Content"，分析该页面源程序，找到提交的变量名，并将该变量名作为Flag提交；

6. 对该任务题目5页面注入点进行渗透测试，使页面DisplayFileCtrl.php回显WebServ2003服务器场景访问日志文件：AppServ/Apache2.2/logs/access.log的内容，并将注入代码作为Flag提交；

7. 进入WebServ2003服务器场景的C:\AppServ\www目录，找到DisplayFileCtrl.php程序，使用EditPlus工具分析并修改PHP源程序，使之可以抵御文件包含渗透测试，并将修改后的源程序中的Flag提交；

8. 再次对该任务题目5页面注入点进行渗透测试，验证此次利用注入点对WebServ2003服务器场景进行文件包含渗透测试无效，并将Web页面回显作为Flag提交。

**（三）第二阶段任务书：分组对抗（30分）**

假定各位选手是某公司的系统管理员，负责服务器（受保护服务器IP、管理员账号见现场发放的参数表）的维护，该服务器可能存在着各种问题和漏洞（见漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多黑客对这台服务器进行攻击。

提示1：该题不需要保存文档；

提示2：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

提示3：加固常规漏洞；

提示4：对其它参赛队系统进行渗透测试，取得FLAG值并提交到裁判服务器。

十五分钟之后，各位选手将真正进入分组对抗环节。

注意事项：

注意1：任何时候不能关闭80端口，否则将判令停止比赛，该阶段分数为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，该阶段分数为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，该阶段分数为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一个。

在这个环节里，各位选手需要继续保护你的服务器免受各类黑客的攻击，你可以继续加固你的服务器，你也可以选择攻击其他组的保护服务器（其他服务器网段见现场发放的参数表）。

漏洞列表：

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存在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系统后门，选手可以找到后门，并利用预留的后门直接获取到系统权限。

选手通过以上的所有漏洞点，最后得到其他选手靶机的最高权限，并获取到其他选手靶机上的FLAG值进行提交。

样题完