**2019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

（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

|  |  |  |  |
| --- | --- | --- | --- |
| 组别 | 专业类 | 专业代码 | 专业名称 |
| 中职 | 信息技术类 | 新增专业 | 网络信息安全 |
| 信息技术类 | 090500 | 计算机网络专业 |
| 信息技术类 | 090100 | 计算机应用专业 |
| 信息技术类 | 090600 | 网站建设与管理专业 |

1. 赛项申报专家组

三、赛项目的

习近平总书记在2018年4月召开的全国网络安全和信息化工作会议上强调：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”，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，护卫我国继陆、海、空、天四个疆域之外的“第五疆域”。

2017年“网络空间安全”赛项的举办直接促进了中职“网络与信息安全”专业的设立，填补了中职领域网络信息安全人才培养的空白。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 “网络与信息安全”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《网络与信息安全专业简介》和《网络与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。

2018年3月，人社部印发《人力资源社会保障部关于颁布<全国技工院校专业目录（2018年修订）>的通知》，开始施行2018版技工院校专业目录，提出0314网络与信息安全专业为信息类新增专业。

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，开赛前一个月公开全部赛题，比赛前随机抽选，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、岗位内容进行设计与整理，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2018年的比赛中，赛项进行了现场直播，效果逼真，实时显示选手得分和排名，页面元素丰富，直观体现竞技过程。可以说，本赛项是国赛中少有的全公开赛项。

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

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。

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。7.6亿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。

（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、山东、浙江、安徽、河南、广东、北京、上海、青岛等80多个省、市级技能大赛；湖北省第二届网络安全技术竞赛；2018年中国技能大赛新疆赛区选拔赛暨第八届自治区职工职业技能大赛；第十八届北京市工业和信息化职业技能竞赛等。平台技术成熟，功能稳定，性能出色，赛题和教学课件注重中职学生特点。

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-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与信息安全专业教学体系，计划配套多本教材，设计开发教学课件，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 Competition

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。

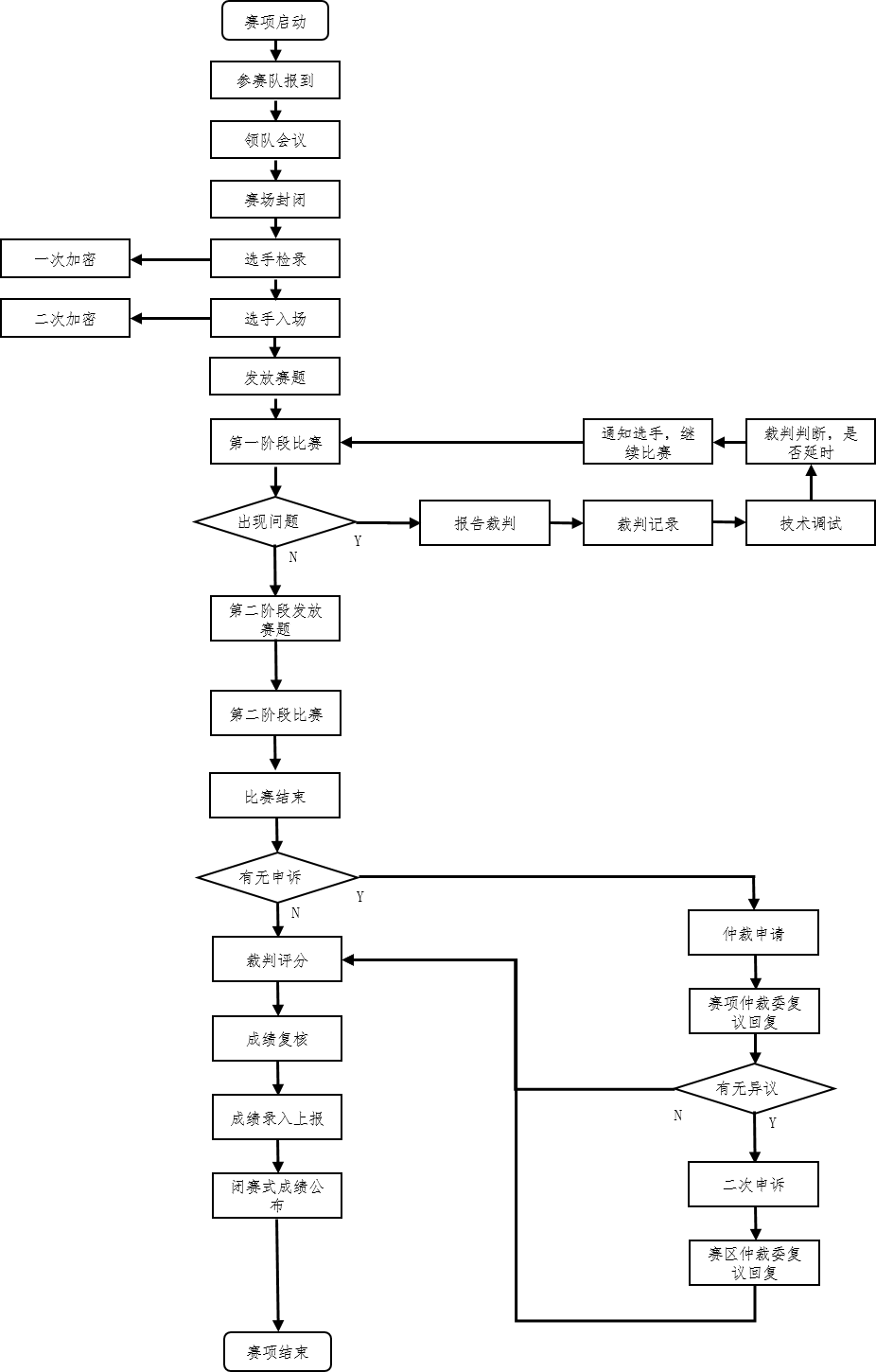
本赛项正在与国际参赛队接洽，同时欢迎国内外团队及选手到场观赛。

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** |
| 赛前2日 | 20:00前 | 裁判、仲裁、监督报到 | 工作人员 | 住宿酒店 |
| 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 |
| 08:30-08:40 | 参赛选手就位，宣读考场纪律 | 参赛选手、裁判 | 竞赛场地 |
| 08:40-09:00 | 设备检查、第一阶段赛题发放 | 参赛选手、裁判 | 竞赛场地 |
| 09:00-10:40 | 第一阶段比赛时间 | 参赛选手、裁判 | 竞赛场地 |
| 10:40-11:00 | 第二阶段赛题发放、攻防准备 | 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 |
| 13:00-18:00 | 成绩核查、解密、确认 | 裁判长、监督 | 竞赛场地 |
| 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

本赛项提供样卷，并且赛项举办两年以上，具有赛题库，赛题库中有12套竞赛赛卷。

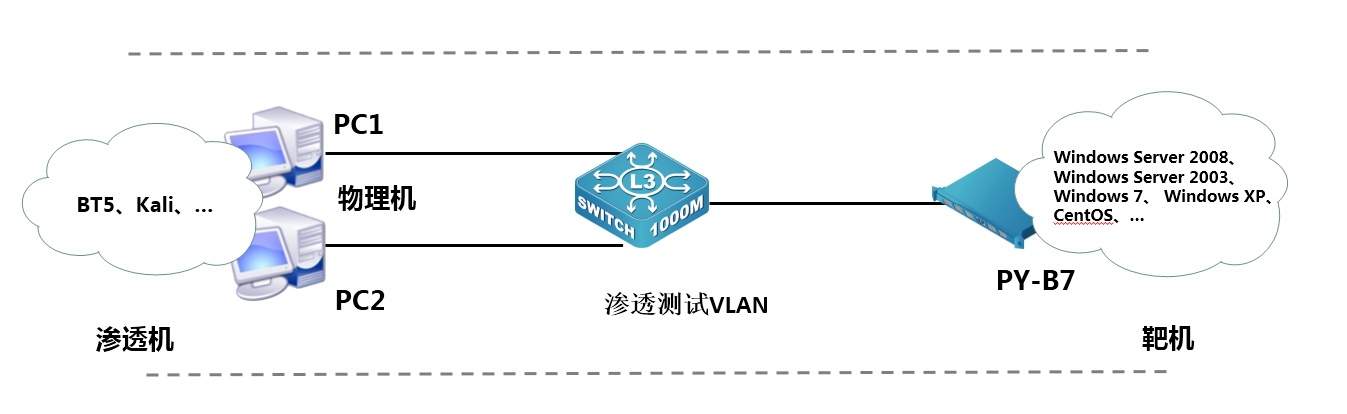
以下为样卷：

**中职组“网络空间安全”赛项样卷**

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 | MSSQL数据库渗透测试 | 100分钟 | 100 |
| 任务2 | 主机发现与信息收集 | 100 |
| 任务3 | SNMP信息收集与利用 | 100 |
| 任务4 | Windows操作系统渗透测试 | 100 |
| 任务5 | Linux操作系统渗透测试 | 100 |
| 任务6 | 网络协议堆栈渗透测试 | 100 |
| 任务7 | Web应用程序渗透测试及安全加固 | 100 |
| 备战阶段 | 攻防对抗准备工作 | | 20分钟 | 0 |
| 第二阶段  分组对抗 | 系统加固：15分钟 | | 60分钟 | 300 |
| 渗透测试：45分钟 | |

二、拓扑图



三、竞赛任务书

（一）第一阶段任务书（700分）

**任务1. MSSQL数据库渗透测试（100分）**

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.在本地PC渗透测试平台BT5中使用zenmap工具扫描服务器场景server2003所在网段(例如：172.16.101.0/24)范围内存活的主机IP地址和指定开放的1433、3306、80端口。并将该操作使用的命令中必须要使用的字符串作为FLAG提交；（10分）

2.通过本地PC中渗透测试平台BT5对服务器场景server2003进行系统服务及版本扫描渗透测试，并将该操作显示结果中数据库服务对应的服务端口信息作为FLAG提交；（10分）

3.在本地PC渗透测试平台BT5中使用MSF中模块对其爆破，使用search命令，并将扫描弱口令模块的名称作为FLAG提交；（10分）

4.在上一题的基础上使用命令调用该模块，并查看需要配置的信息（使用show options命令），将回显中需要配置的目标地址,密码使用的猜解字典,线程,账户配置参数的字段作为FLAG提交（之间以英文逗号分隔，例hello,test，..,..）；（10分）

5.在msf模块中配置目标靶机IP地址，将配置命令中的前两个单词作为FLAG提交；（10分）

6.在msf模块中指定密码字典，字典路径为/root/2.txt爆破获取密码并将得到的密码作为FLAG提交；（14分）

7.在msf模块中切换新的渗透模块，对服务器场景server2003进行数据库服务扩展存储过程进行利用，将调用该模块的命令作为FLAG提交；（14分）

8.在上一题的基础上，使用第6题获取到的密码并进行提权，同时使用show options命令查看需要的配置，并配置CMD参数来查看系统用户，将配置的命令作为FLAG提交；（14分）

9.在利用msf模块获取系统权限并查看目标系统的异常（黑客）用户，并将该用户作为FLAG提交。（8分）

**任务2. 主机发现与信息收集（100分）**

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.通过本地PC中渗透测试平台BT5使用fping对服务器场景server2003所在网段(例如：172.16.101.0/24)进行主机发现扫描,并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

2.通过本地PC中渗透测试平台BT5使用genlist对服务器场景server2003所在网段进行扫描进行主机存活发现, 并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

3.在通过本地PC中渗透测试平台BT5使用nbtscan对服务器场景server2003所在网段进搜索扫描，获取目标的MAC地址等信息，并将该操作使用的命令中必须要使用的参数作为FLAG提交；（12分）

4.假设服务器场景server2003设置了防火墙无法进行ping检测，通过PC中渗透测试平台BT5使用arping检测主机连通性扫描（发送请求数据包数量为4个），并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

5.通过本地PC中渗透测试平台BT5使用fping对服务器场景server2003所在网段进行存活性扫描，且要把最终扫描的存活主机输出到文件ip.txt中，并将该操作使用的命令中必须要使用的参数作为FLAG提交（各参数之间用英文逗号分割，例a,b）；（12分）

6.通过本地PC中渗透测试平台BT5使用nbtscan从第5题的ip.txt文件中读取IP扫描主机信息MAC地址等信息，并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

7.通过本地PC中渗透测试平台BT5使用xprobe2对服务器场景server2003进行TCP扫描，仅扫描靶机80,3306端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为FLAG提交；（12分）

8.通过本地PC中渗透测试平台BT5使用xprobe2对服务器场景server2003进行UDP扫描，仅扫描靶机161,162端口的开放情况(端口之间以英文格式下逗号分隔)，并将该操作使用的命令中固定不变的字符串作为FLAG提交。（16分）

**任务3. SNMP信息收集与利用（100分）**

**任务环境说明：**

* 服务器场景：server2003（用户名：administrator；密码：空）
* 服务器场景操作系统：Windows server2003

1.在本地PC渗透测试平台BT5中使用autoscan工具扫描服务器场景server2003所在网段(例如：172.16.101.0/24)范围内存活的主机地址。判断存活主机是否开放网络管理服务，若开启则以扫描出开启SNMP服务的主机名作为FLAG提交；（11分）

2.在本地PC渗透测试平台BT5中使用nmap工具进行UDP扫描服务器场景server2003所在网段范围内存活的主机地址，判断网络管理服务的开放情况，若开启，则以扫描出SNMP开放的端口号作为FLAG（各端口之间用英文分号分割，例21;23），若未开放则提交none作为FLAG；（11分）

3.在本地PC渗透测试平台BT5中调用snmpwalk工具测试服务器场景server2003是否开启Windows SNMP服务（共同体为默认字符串为public，通过对目标靶机的.1.3.6.1.2.1.25.1.6分支进行snmpwalk来测试服务的开放情况（SNMP 版本为v2c），并将该操作使用的命令中必须要使用的参数作为FLAG提交（各参数之间用英文分号分割，例a;b）；（11分）

4.在本地PC渗透测试平台BT5中使用ADMsnmp工具尝试猜解团体字符串，并将使用的全部命令作为FLAG提交（提交答案时IP以192.168.100.10代替,使用默认字典snmp.passwd）；（11分）

5.更换使用onesixtyone工具执行命令查看帮助选项，并将输入的命令作为FLAG提交；（11分）

6.在本地PC渗透测试平台BT5中使用onesixtyone对靶机SNMP进行团体字符串猜解，并将使用的全部命令作为FLAG提交（提交的命令为忽略IP后必须使用的命令，字典名字为dict.txt）；（11分）

7.在本地PC渗透测试平台BT5中对猜解结果进行查看，将回显中猜解的团体字符串作为FLAG提交；（11分）

8.在本地PC渗透测试平台BT5中选择新的SNMP攻击模块snmpcheck，根据得到的public团体字符串并利用snmpcheck进行对靶机的信息收集，并将该操作使用的命令中必须使用的参数作为FLAG提交；（11分）

9.查看获取的系统信息，将系统管理员用户和异常（黑客）用户作为FLAG提交，（各用户之间用英文分号分割，例root;user）。（12分）

**任务4. Windows操作系统渗透测试（100分）**

**任务环境说明：**

* 服务器场景：PYsystem4
* 服务器场景操作系统：Windows（版本不详）

1.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行操作系统扫描渗透测试，并将该操作显示结果“Running：”之后的字符串作为FLAG提交；（6分）

2.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行系统服务及版本扫描渗透测试，并将该操作显示结果中445端口对应的服务版本信息字符串作为FLAG提交；（6分）

3.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景网络连接信息中的DNS信息作为FLAG提交;(例如114.114.114.114)（13分）

4.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景桌面上111文件夹中唯一一个后缀为.docx文件的文件名称作为FLAG提交；（14分）

5.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景桌面上111文件夹中唯一一个后缀为.docx文件的文档内容作为FLAG提交；（16分）

6.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景桌面上222文件夹中唯一一个图片中的英文单词作为FLAG提交；（15分）

7.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景中的当前最高账户管理员的密码作为FLAG提交；（10分）

8.通过本地PC中渗透测试平台Kali对服务器场景PYsystem4进行渗透测试，将该场景中回收站内文件的文档内容作为FLAG提交。（20分）

**任务5. Linux操作系统渗透测试（100分）**

**任务环境说明：**

* 服务器场景：PYsystem5
* 服务器场景操作系统：未知

1.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行操作系统扫描渗透测试，并将该操作显示结果“OS Details：”之后的字符串作为FLAG提交；（6分）

2.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行系统服务及版本扫描渗透测试，并将该操作显示结果中MySQL数据库对应的服务版本信息字符串作为FLAG提交；（6分）

3.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文件名称作为FLAG提交；（12分）

4.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/var/www/html目录中唯一一个后缀为.html文件的文件内容作为FLAG提交；（16分）

5.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/root目录中唯一一个后缀为.bmp文件的文件名称作为FLAG提交；（27分）

6.通过本地PC中渗透测试平台Kali对服务器场景PYsystem5进行渗透测试，将该场景/root目录中唯一一个后缀为.bmp的图片文件中的英文单词作为FLAG提交。（33分）

**任务6. 网络协议堆栈渗透测试（100分）**

**任务环境说明：**

服务器场景：WindowsServer18065

服务器场景操作系统：Windows2003 Server

服务器场景FTP下载服务用户名：anonymous，密码：123456

服务器场景FTP下载服务端口：2121

1.通过物理机的ping程序访问靶机，成功访问后，在攻击机中使用arpspoof程序对物理机进行ARP渗透测试，对物理机进行ARP缓存毒化为：靶机IP地址映射攻击机MAC地址；从靶机服务器场景的FTP服务器中下载文件arpspoof.py，编辑该Python3程序文件，使该程序实现同本任务中arpspoof程序一致的功能，填写该文件当中空缺的F1字符串，将该字符串作为Flag值提交；（9分）

2.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F2字符串，将该字符串作为Flag值提交；（9分）

3.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F3字符串，将该字符串作为Flag值提交；（9分）

4.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F4字符串，将该字符串作为Flag值提交；（9分）

5.继续编辑该Python3程序文件，使该程序实现同本任务题1中arpspoof程序一致的功能，填写该文件当中空缺的F5字符串，将该字符串作为Flag值提交；（9分）

6.继续从靶机服务器场景FTP服务器中下载文件icmpflood.py，编辑该Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F6字符串，将该字符串作为Flag值提交；（9分）

7.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F7字符串，将该字符串作为Flag值提交；（9分）

8.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F8字符串，将该字符串作为Flag值提交；（9分）

9.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F9字符串，将该字符串作为Flag值提交；（9分）

10.继续编辑命名为icmpflood.py的Python3程序文件，使该程序实现通过ICMP对物理机进行DOS（拒绝服务）渗透测试的功能，填写该文件当中空缺的F10字符串，将该字符串作为Flag值提交；（9分）

11. 在本地PC渗透测试平台BT5中通过Python3程序解释器执行程序文件icmpflood.py，并打开WireShark监听网络流量，分析通过程序文件icmpflood.py产生的ICMP流量，并将该ICMP数据对象中的Code属性值通过MD5运算后返回的哈希值的十六进制结果的字符串作为Flag值提交。（10分）

**任务7. Web应用程序渗透测试及安全加固（100分）**

**任务环境说明：**

服务器场景：WindowsServer18065

服务器场景操作系统：Windows2003 Server

服务器场景FTP下载服务用户名：anonymous，密码：123456

服务器场景FTP下载服务端口：2121

服务器场景FTP上传服务用户名：anonymous，密码：123456

服务器场景FTP上传服务端口：21

1.在攻击机端通过浏览器访问主页http://靶机IP地址，通过Web应用程序渗透测试方法登陆磐石公司模拟产品网站，成功登陆后，将Web页面弹出的字符串通过SHA256运算后返回哈希值的十六进制结果的字符串作为Flag值提交；（7分）

2.从靶机服务器场景FTP服务器中下载文件loginauthentic.php，编辑该PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F11字符串，将该字符串作为Flag值提交；（7分）

3.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F12字符串，将该字符串作为Flag值提交；（7分）

4.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F13字符串，将该字符串作为Flag值提交；（7分）

5.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F14字符串，将该字符串作为Flag值提交；（7分）

6.继续编辑本任务第2题中的PHP程序文件，使该程序实现能够对本任务第1题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F15字符串，将该字符串作为Flag值提交；（7分）

7.将编辑好后的loginauthentic.php程序文件上传至靶机FTP服务，在攻击机端通过浏览器访问主页http://靶机IP地址，通过本任务第1题所使用的Web应用程序渗透测试方法登陆磐石公司模拟产品网站，将此时Web页面弹出的字符串通过SHA256运算后返回的哈希值的十六进制结果的字符串作为Flag值提交；（7分）

8.成功登陆磐石公司模拟产品网站后，继续点击超链接进入磐石公司产品信息页面，通过Web应用程序渗透测试方法获得靶机根路径下的文件flaginfo中的字符串，并将该字符串通过SHA256运算后返回哈希值的十六进制结果的字符串作为Flag值提交；（8分）

9.从靶机服务器场景FTP服务器中下载文件product.php，编辑该PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F16字符串，将该字符串作为Flag值提交；（7分）

10.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F17字符串，将该字符串作为Flag值提交；（7分）

11.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F18字符串，将该字符串作为Flag值提交；（7分）

12.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F19字符串，将该字符串作为Flag值提交；（7分）

13.继续编辑本任务第9题中的PHP程序文件，使该程序实现能够对本任务第8题中的Web应用程序渗透测试过程进行安全防护，填写该文件当中空缺的F20字符串，将该字符串作为Flag值提交；（7分）

14.将编辑好后的product.php程序文件上传至靶机FTP服务，并在攻击机端通过本任务第8题中使用的Web应用程序渗透测试方法获得靶机根路径下的文件flaginfo中的字符串，将此时Web页面弹出的字符串通过SHA256运算后返回的哈希值的十六进制结果的字符串作为Flag值提交。（8分）

（二）第二阶段任务书（300分）

假定各位选手是某电子商务企业的信息安全工程师，负责企业某些服务器的安全防护，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些服务器进行渗透。

根据《赛场参数表》提供的第二阶段的信息，请使用PC的谷歌浏览器登录实战平台。

**靶机服务器环境说明：**

场景1：CentOS2018065（用户名：root；密码：123456），服务器操作系统：CentOS（版本不详）；

场景2：Windows2018065（无法打开控制台操作该靶机，只能获取到该靶机的IP，选手需要通过其他方法进入靶机才能进行加固），服务器场景操作系统：Windows（版本不详）。

**注意事项：**

1.不能对裁判服务器进行攻击，警告一次后若继续攻击将判令该参赛队离场；

2.FLAG值为每台靶机服务器的唯一性标识，每台靶机服务器仅有1个；

3.靶机服务器的FLAG值存放在/root/flagvalue.txt文件或C:\ flagvalue.txt文件中；

4.在登录自动评分系统后，提交对手靶机服务器的FLAG值，同时需要指定对手靶机服务器的IP地址；

5. CentOS2018065靶机服务器如下服务及端口不允许关闭：21、22、23、80、555、3306、7000-7999；Windows2018065靶机服务器如下服务及端口不允许关闭：HTTP 80、FTP 21、Telnet 23、7000-7999；

6.系统加固时需要保证靶机对外提供服务的可用性，服务只能更改配置，不允许更改内容；

7.本环节是对抗环节，不予补时。

**可能的漏洞列表如下：**

1.服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

2.靶机服务器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;

3.靶机服务器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;

4.靶机服务器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;

5.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;

6.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;

7.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。

**评分说明：**

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

规则2：系统自动启动违规检测和扣分机制，如发现如下违规行为，系统均给予自动扣分，每检测到一次违规行为扣除一次分数，扣分明细显示在违规记录中，计算在第二阶段总成绩中：

1）攻防阶段启用FLAG检测机制，如发现FLAG异常（譬如：删除、修改、移动、杀进程），记为一次违规行为，每次扣分3分；

2）攻防阶段启用服务端口检测机制，如发现关闭题目要求开启的端口，记为一次违规行为，每端口每次扣分1分；

3）攻防阶段靶机服务器IP地址为DHCP自动获取，不允许修改，如修改触发上述所有检测机制；

4）在加固时间后，选手自己关闭靶机服务器或被他人关闭，触发上述所有检测机制，且裁判员不予帮助重启。

（样卷完）

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1000分，分为两个阶段单独积分，第一阶段满分为700分，第二阶段满分为300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，由裁判长汇总整理各阶段得分得出各参赛队总分和总排名，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

第一阶段分为多个任务，每个任务里面有多个关卡，占总分比例为70%；第二阶段占总分比例为30%。

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。

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 |

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.自动评分规则

（1）第一阶段评分规则

规则1：系统自动评分和排名，显示在大屏幕上；

规则2：同分的选手会根据系统提供的答题时间进行排名，答题时间为最后一个正确FLAG值提交的时间，先提交者排名靠前。

（2）第二阶段评分规则

规则1：第二阶段根据题目要求设定初始100分，每提交1次对手靶机的FLAG值加分，每当被对手提交1次自身靶机的FLAG值扣分，每个对手的每个靶机FLAG值只能提交一次；

规则2：选手的“实际得分”显示在大屏，某选手“实际得分”可能会显示负分或者超过上限300分；凡是负分的，本阶段“评判成绩”一律为0分；凡是超过300分的，本阶段“评判成绩”一律为300分计算；选手成绩排名次序保持不变，得分相同的选手根据“实际得分”以及得分时间点不同而排名不同。

【名辞解释】

实际成绩：这是系统自动打出的分数，会显示在大屏幕上，分数可能是负数，可能是超过第二阶段满分300分的分数；

评判成绩：0-300分之间，是裁判长根据系统导出的成绩进行修订，保证第二阶段成绩不影响其他阶段成绩。

4.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。

5.违规扣分原则

第二阶段系统自动启动违规检测和扣分机制，如发现如下违规行为，系统均给予自动扣分：

规则1：攻防阶段启用FLAG检测机制，如发现靶机FLAG异常（譬如：删除、修改、杀进程），记为一次违规行为，随机检测，循环扣分；  
 规则2：攻防阶段启用服务端口检测机制，如发现关闭题目要求开启的端口，记为一次违规行为，随机检测，循环扣分；  
 规则3：攻防阶段靶机服务器IP地址为DHCP自动获取，不允许修改，如修改触发上述所有检测机制；

规则4：在加固时间后，选手自己关闭靶机或被他人关闭，触发上述所有检测机制，且裁判员不予帮助重启。

6.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%，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** | **设备描述** |
| 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。包含往年网络空间安全国赛和省赛赛题场景。 |
| 2 | PC机 | 2台/赛位 | CPU 主频>=3.2GHZ,>=四核四线程；内存>=8G；硬盘>=500G；支持硬件虚拟化；支持同传。 |

（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(64位中文版)试用版

2.虚拟机安装操作系统：

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

3.其他应用软件：

（1）VMware workstation 12 pro 免费版

（2）Putty 0.67.0.0

（3）Python 3

（4）Chrome 浏览器 62.0

（5）RealVNC 客户端 4.6

（6）JDK（Java Development Kit）7.0

（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。

（五）赛项可靠性设计：

1．电力系统可靠性设计

供电负荷匹配电力要求，防止电子设备运行过程中过载导致火灾隐患或电力中断；提供三项电源接地保证，杜绝运行过程中静电可能导致设备重启、短路、漏电等安全威胁；布线强弱电分离，防止发生干扰；各区域供电保障独立，相互不干扰。

2．弱电系统可靠性设计

弱电系统必须保证良好的运行状态，系统应具备长期和稳定的工作能力，遇到突发状况时应存在快速解决方法，保证系统可靠运行。弱点系统应与电力系统隔离部署，防止干扰造成故障。

3．网络设备可靠性设计

网络设备必须要运行稳定，满足带宽要求，预留端口备份，通信线缆、设备预留备份，具备故障快速恢复机制，提供必要的冗余备份设计。

4．攻防平台可靠性设计

平台必须支持集群功能，在大规模流量下支持负载分担，同时可为竞赛数据提供备份、回退机制。具备冗余备份机制，在最短时间内恢复故障问题。平台应提供访问控制机制，具备防攻击手段，保障平台运行稳定。

5．PC可靠性设计

PC的部署必须保证良好的运行状态，遇到突发状况时应存在快速解决方法，保证系统可靠运行。系统规格必须满足要求，保证良好的性能和稳定的运行。

（六）系统故障的应急处理方案

1．参赛选手PC故障

如参赛选手PC遇到故障，先判断其为硬件故障还是软件故障。软件故障对PC进行重启，因PC配备还原卡，可将系统恢复至初始状态，故障恢复时间30秒；硬件故障经过现场裁判允许后对更换备用机，故障恢复时间1分钟。键盘、鼠标故障及时更换，恢复时间1~3分钟。

2．竞赛工位线缆连接故障

竞赛工位如遇到网络连接问题，因选手设置操作问题不出来，线缆物理连接问题，及时更换备用线缆，故障恢复时间15秒；竞赛工位两条以上网线物理故障，经现场裁判允许为其更换竞赛工位，故障恢复时间3~5分钟。

3．竞赛工位电力故障

如遇竞赛工位电力故障，经裁判长允许更换备用工位。故障恢复时间3~5分钟。

4．网络设备交换机故障

更换备用交换机，部分影响，故障恢复时间5~10分钟；跳线线缆故障及时更换备用线缆（光纤及网线）。部分影响，故障恢复时间3~5分钟。

5．攻防平台集群故障

服务器集群主设备故障，启用备用集群设备，数据有备份，集群恢复时间5~10分钟。服务器集群从设备故障，更换备用设备，恢复时间5~10分钟。

6．WEB应用防火墙故障

如遇WAF设备故障，影响访问，取消防护策略或取消WAF设备连接，故障恢复时间1~3分钟。

7．服务器区供电问题

若服务器区发生供电问题，UPS电源可支持20~30分钟。

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。

5、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

在大赛执委会的领导与监督下，赛后30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：

（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，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。

（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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **资源名称** | | | **表现形式** | **资源数量** | **资源要求** | **完成时间** | **实施人员** |
| 基 本 资 源 | 风采 展示 | 赛项宣传片 | 视频 | 1 | 15 分钟  以上 | 赛后5日 | 承办校 |
| 风采展示片 | 视频 | 1 | 10 分钟  以上 | 赛后5日 | 承办校 |
| 技能 概要 | 技能介绍 | 文本 | 1 | 补充完善 | 赛后60日 | 专家组 |
| 训练大纲 | 文本 | 1 | 补充完善 | 赛后60日 | 专家组 |
| 评价指标 | 文本 | 1 | 补充完善 | 赛后60日 | 专家组 |
| 教学 资源 | 专业教材 | 教材 | 1 | 电子教材 | 赛后90日 | 专家组  技术支持单位 |
| 技能训练  指导书 | 教材 | 1 | 电子教材 | 赛后90日 | 专家组  技术支持单位 |
| 拓 展 资 源 | 赛题库 | | 文本 | 2套 |  | 赛后90日 | 专家组  技术支持单位 |
| 优秀选手访谈 | | 视频 | 1 |  | 赛后90日 | 承办校 |

十八、筹备工作进度时间表

|  |  |  |
| --- | --- | --- |
| **序号** | **时间** | **事项** |
| 1 | 2018年8月 | 组建赛项申报专家组，编写申报材料 |
| 2 | 2018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 | 2018年12月 | 赛事技术文件网上预发布  确定比赛场地 |
| 4 | 2019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 | 2019年3月初 | 讨论国赛试题  参赛队报名 |
| 6 | 2019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 | 2019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 | 2019年4月初 | 所有赛项文件汇总报秘书处 |
| 9 | 2019年4月10日 | 确定命题人选  设备、器材、用品全部到位 |
| 10 | 2019年4月15日 | 现场启动 |
| 11 | 2019年4月15-22日 | 考题确定  比赛设备安装与调试 |
| 12 | 2019年4月23日 | 启动正式比赛流程 |
| 13 | 2019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

按照《全国职业院校技能大赛专家和裁判工作管理办法》的有关要求，详细列出赛项所需现场裁判和评分裁判的具体要求。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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、赛题公开承诺

本赛项承诺保证于开赛1个月前在大赛网络信息发布平台上（www.chinaskills-jsw.org)公开全部赛题。

二十一、其他