**2018年全国职业院校技能大赛**

**赛项申报书**

赛项名称：信息安全管理与评估

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：电子信息大类

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教学工作委员会

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28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

信息安全管理与评估（2017-2020规划赛项）

（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

61电子信息大类

6102计算机类

610211信息安全与管理

**二、赛项申报专家组**

**三、赛项目的**

（一）检验教学成果

全国信息安全与管理和计算机网络技术的专业点数已经超过700多个，在校生40多万，2018年大赛是延续历届信息安全赛项的竞赛内容，通过赛项检验参赛选手网络组建、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

针对国家“十二五”期间互联网+、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》的信息安全技术专业建设框架，通过赛项丰富完善学习领域课程建设，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”、“操作系统安全”等7门核心课程内容。

（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，赛前完成竞赛内容向教学改革的成果转化，实现以赛促教、以赛促学、以赛促改的教产合作赛事创新。

**四、赛项设计原则**

（一）坚持公开、公平、公正

为保证竞赛公平、公开、公正，本赛项汇集大量国赛及各省市赛的样题、赛题。每年比赛来源于以专家组、国家示范校、行业专家、企业专家为班底成立赛题开发团队，参照行业规范，工作内容，设计比赛试题。

同时大赛设计与国际接轨，在竞赛前即会发布竞赛设备和设备技术文档，竞赛设计的网络环境等竞赛相关信息，参赛选手可以有充分的时间思考网络架构、查找网络资料、针对性训练，得到水平迅速提高；在实际竞赛中，基于已经发布的网络环境，选手可对竞赛试题中具体的技术问题借助设备技术文档进行设计和解决，通过开放的形式扩大了竞赛的公平性，保证了真实工作实践相符合，充分考察学生整体运用知识的能力。

（二）赛项涉及专业面宽，受益面广

该赛项不仅信息安全与管理专业的学生可以参加比赛，而且其他相关专业也非常适合参加，具体包括：610201计算机应用技术、610202计算机网络技术、610203计算机信息管理、610204计算机系统与维护、680705K司法信息安全等专业的学生都适合参加该赛项。

职业院校开设专业点多，全国仅信息安全技术和网络技术的专业点数已经超过700多个，在校生超过40多万。

（三）竞赛内容涉及岗位群广泛，社会认同度高

赛项内容高度覆盖了信息安全与管理专业、计算机网络专业等职业岗位或岗位群技能要求，对信息安全技术支持工程师、信息安全产品销售工程师、计算机网络工程师、网络安全运维工程师等专业人才岗位技能培养吻合度高，成为专业岗位群人才培养的重要抓手。

通过竞赛展示电子信息大类计算机类学生的信息安全实践能力，全面提升信息安全意识，促进社会对信息安全相关岗位的了解，提高学生的就业质量和就业水平。

赛项围绕企业信息安全的实际需求和岗位要求进行设计，通过竞赛促进相关课程、教材、师资、证书、就业等全面建设，引领相关专业课程改革创新。赛项紧扣信息安全最新技术和当前核心应用领域设计，通过赛项提高教师和学生的信息安全管控能力，提升学生从事信息安全相关岗位的适岗性，为“互联网+”国家战略和国家“智慧城市”规划提供信息安全领域的技能型精英人才。

（四）赛项设计关注新技术和新产业需求，体现与时俱进

赛项设计瞄准国家战略产业发展需求和信息安全技术的发展趋势以及行业部署，重点关注“互联网+”和“云计算”等产业实施过程中数据安全。赛项以信息安全为主题，引入数据中心网络安全、系统安全和网站安全技术，符合新一轮信息产业发展要求。通过任务驱动方式，重点考核参赛选手对数据挖掘、分析、监管与保护等网络空间安全的技术，旨在培养高职相关专业学生胜任信息安全核心岗位的能力。

根据国家十三规划纲要，城镇热点公共区域推广免费高速无线局域网，无线网络技术将成为新的技术趋势，因此将无线网络技术相关知识点加入到赛项中，主要涉及无线网络的基本搭建，支持IEEE 802.11n最新的无线高速接入技术，无线网络安全，包括多种认证和加密机制，如WEP、WPA、MAC地址准入控制等技术。本赛项所设计的无线网络技术可以作为学校信息安全和网络技术专业课程内容中的补充内容，可以帮助完善该专业的课程资源。

2017年5月“WannaCry”漏洞爆发，波及100余个国家超过30万台终端，该病毒是一种“蠕虫式”勒索病毒，给中毒用户带来巨大的经济损失。在网络安全事件层出不穷的今天，我们需要用更新更全面的防御方式来应对新网络环境下的安全威胁，因此我们将入侵检测系统加入到赛项中，入侵检测系统可以全面深入到2-7层进行分析和检测，防御传统的ARP攻击、DDOS攻击的同时，可以实时阻断网络流量中隐藏的病毒、蠕虫、木马、溢出攻击等恶意行为；站在应用的视角，将应用中的异常行为、异常流量也做为威胁的一种做有效的防护，对于未知的威胁以及日益盛行的高级持续威胁会送往云端进一步分析，形成对网络基础设施、网络应用、网络性能、云端安全的全面立体防护。

赛事具有良好的延续性。赛项设计兼容历年信息安全赛项并有所创新和突破，从单纯的组网到安全加固，再发展到系统安全评估与运维管控，2018年信息安全管理与评估赛项延续历届赛事经验，加强对系统和安全防护的比重，使赛项更大范围符合社会岗位需求和贴近行业需要。

（五）竞赛平台成熟，赛项举办经验丰富

采用的设备大部分为往届技能大赛设备，并且在职业院校的实验室已经有广泛应用。

同时与其他赛项相比，赛项牵头单位和赞助企业等各方无论在赛事组织、生活保障、安全管控上都具有丰富的办赛经验。

**五、赛项方案的特色与创新点**

（一）协同性

赛项方案强调多个协同：一是学员之间相互协同。即学员之间既有分工也有合作，协同作战，强调团队协同；二是教与学相互协同。高职教学要求按照其自身的目标、结构和功能，必须循序、系统、连贯的进行。通过大赛的平台，让教师知道教什么，让学生知道学什么，可以改变过去只注重教师的“教”，而忽略学生的“学”的现象，使以教师为主导的“教”与以学生为主题的“学”两个方面有机统一起来，相互激励，共同进步，提高学生的综合素质及创新能力。三是以大赛项目为目标的教学过程，使教师和学生不再是主动与被动的关系，而是双方共同投身于教学之中，各自敞开自我、接纳彼此，相互配合、共同参与教学活动。

同时，大赛对网络安全、信息系统安全、网站安全等技术内容的考核，既不完全脱离专业教学，又以专业教学为基础，相互促进，相互协同。

（二）公平性

赛项设计了分组对抗环节，分组对抗环节所要保护的正是前一个阶段学员自己所加固的服务器中的一个，再通过调整环境的不可确定性（分组、IP分配等因素），使得现场可以很好的调节因素，规避因为赛题带来的保密性问题，比赛成绩完全取决于学员的真实水平和应变能力。

2017年开始赛项专门设计了竞赛评价系统，70%的比赛计分将采用计算机系统自动评分模式，保障大赛计分的准确度与实时性，并且可以做到与场外大屏实时显示各参赛队比赛得分情况，最大限度的保障赛事的公开、公平与公正。

（三）趣味性和观赏性

赛项研发设计了场内攻防实时显示系统，在比赛的第二阶段和第三阶段将各个参赛队的攻击过程实时显示，通过大屏幕等醒目的方式将场内进程直接展示在指导教师休息区，让各个参赛队伍的指导老师可以直接看到攻击过程，提高参与度。同时还将各个参赛队伍的成绩和实时排名也展示出来，实现了趣味性、观赏性、竞技性的有效结合。

场外的指导教师实时掌握场内竞赛选手的比赛状况，不仅仅是观赏，还可以进行记录选手比赛中的得与失，便于赛后的复盘。这种复盘的训练将会对于后续的备赛和纳入教学体系都有着很好的借鉴意义。

（四）对接产业，紧扣经济发展，培养专业人才

信息安全已上升为国家战略，没有信息安全就没有国家安全，依照目前安全行业在整个经济环境下发展形态，以及信息安全在经济发展中的重要程度，赛项所匹配的岗位是目前信息安全行业中人才需求较为紧缺的岗位，也是高职信息安全人才培养的重点方向，符合信息安全行业发展在社会经济体中的定位，赛项强调的数据安全、计算机取证、风险评估能力，无线网络安全等方面与实际用人需求完全吻合。

（五）以赛促改，推进竞赛成果向教学资源转化。

2018年信安赛项通过教产合作，基于工作过程，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。在前几届比赛的基础上，完善了教学体系，已经配套了多本“十二五”规划教材，并且设计了交互式实训课件辅助教学。

（六）延续发展，逐年提升赛项品质。

赛项采用国际和国家标准设计，面向国际化接轨；竞赛内容逐年延续、渐进发展，不断引领专业建设与人才培养；竞赛器材向前兼容，适度增加，减轻学校参赛负担。

**六、竞赛内容简介（须附英文对照简介）**

“信息安全管理与评估”项目竞赛设计遵循《2017年全国职业院校技能大赛制度汇编》的总体指导思想及原则。

竞赛设计适应国家产业结构调整与社会发展需要，展示知识经济时代高技能人才培养的特点，聚焦信息安全技术应用领域岗位的主要技能，与相关企业紧密合作，以实际项目为基础，针对计算机网络专业学生的“能力短板”，围绕信息安全技术应用领域的先进技术、主流产品，力求突出面向应用的技能培养；着重考查选手面向应用的网络安全能力、系统安全能力、网站安全能力职业道德、组织管理能力、工作计划性和团队协作精神，以赛促教，以赛促改，引领信息安全与管理专业的教育教学改革；通过竞赛展示高职院校信息安全与管理专业学生的面向应用实践能力，促进社会对面向应用网络信息安全工程相关岗位的了解，提高高职院校信息安全与管理专业的社会认可度，提高学生的就业质量和就业水平。

竞赛的设计面向信息安全管理与评估领域的主要岗位及其所需技能，突出信息安全技术领域的应用，体现面向应用信息安全领域的先进技术，强调引领教学改革，并积极借鉴世界技能大赛（World Skills）的竞赛内容、形式和规则。

The design of competition should adapt to the management of national industries' structure and the need of social development, to present the characteristic of talented people trained in knowledge economy period, to focus on the main skills of information and security technique application’s domain; and the competition also needs to collaborate with enterprises closely, which are based on the real projects, aim at the students of 'skill shortcoming' in computer networks major, and depends on advanced technique, mainstream products to highlight the skill training via facing to application. It examines every player's ability of application about network security, system security, website security, professional ethics, management of organizing, working arrangement and the spirit of teamwork. It also accelerates teaching quality, accelerates teaching innovation; to present college students' practice in network security major, to make community understand more on jobs of network security, and to improve the community's recognition of information security major in profession academies, obtaining employment and it's quality.  
 The competition's design should face to main jobs and skills in the domain of application of information security technique, and should highlight the application of information security, advanced skills and lead of teaching innovation, and should refer to World Skills Competition's content, format and rules.

**七、竞赛方式（含组队要求、是否邀请境外代表队参赛）**

（一）竞赛以团队方式进行，每支参赛队由3名选手组成，须为同校在籍学生，其中队长1名，性别和年级不限，可配2名指导教师。

参赛选手为2018年在籍的高职学生，性别不限，年龄不超过25周岁。

（二）竞赛分预赛和决赛两个阶段。

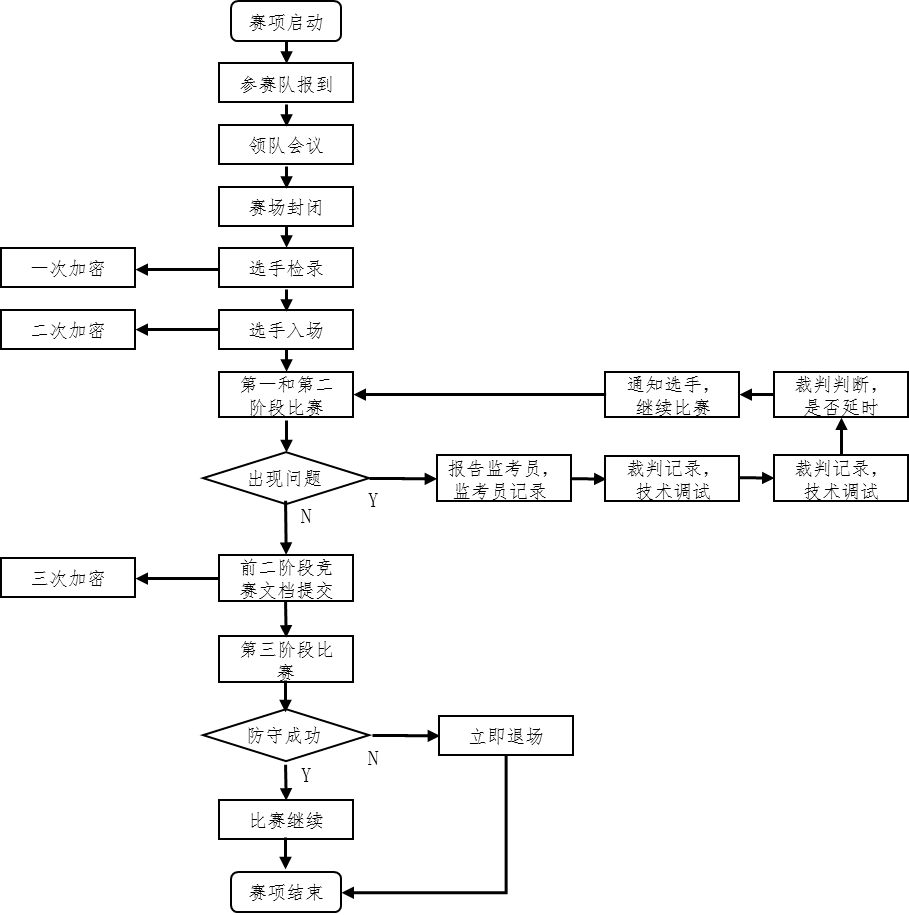
预赛由各省、自治区、直辖市，各计划单列市以及新疆建设兵团等有关部门自行组织，决赛由2018年全国职业院校技能大赛组委会统一组织。

（三）参赛规模。

决赛参赛队由各省、自治区、直辖市，各计划单列市以及新疆建设兵团等有关部门推荐，根据决赛队数量决定是否分组进行。

（四）暂不邀请境外代表队参赛。

**八、竞赛时间安排与流程**

（一）竞赛流程图

（二）竞赛时间表

比赛限定在1天内进行，赛项竞赛时间为6小时，时间为9:00-15:00，具体安排如下：

|  |  |
| --- | --- |
| **日程安排** | |
| 07:30 | 裁判进入裁判室 |
| 08:00-08:30 | 选手抽签，一次加密 |
| 08:30-08:50 | 选手抽签，二次加密及入场 |
| 08:50-09:00 | 参赛代表队就位，宣读考场纪律 |
| 09:00-09:15 | 第一阶段和第二阶段赛题发放时间 |
| 09:15-13:30 | 第一阶段和第二阶段正式比赛时间 |
| 13:30-14:00 | 第一阶段与第二阶段比赛结果提交时间，三次加密 |
| 14:00-14:15 | 第三阶段赛题发放时间 |
| 14:15-15:00 | 第三阶段正式比赛时间 |
| 15:00 | 比赛正式结束 |

备注：参赛选手午餐时间由大赛组委会统一安排，就餐时间计入比赛时间。

**九、竞赛试题**

**2018年全国职业院校技能大赛高职组**

**信息安全管理与评估赛项任务书（样题）**

一、赛项时间

9:00-13:00，共计6小时，含赛题发放、收卷及午餐时间。

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  平台搭建与配置 | 任务一 | 网络平台搭建 | 9:00-13:30 | 60 |
| 任务二 | 网络安全设备配置与防护 | 240 |
| 第二阶段  系统安全攻防及运维安全管控 | 任务一 | 缓冲区溢出漏洞渗透测试 | 400 |
| 任务二 | Web应用程序安全攻防 |
| 任务三 | ARP扫描渗透测试 |
| 任务四 | 操作系统判断渗透测试 |
| 任务五 | 数据库访问渗透测试及其加固 |
| 任务六 | 网络协议渗透测试及其加固 |
| 中场收卷 | | | 13:30-14:00 | |
| 第三阶段  分组对抗 | 系统加固 | | 14:00-14:15 | 100 |
| 系统攻防 | | 14:15-15:00 | 200 |

三、赛项内容

假定各位选手是某公司的信息安全工程师，负责维护公司信息系统安全。你们需要完成三个阶段的任务，其中前两个阶段需要提交任务操作文档留存备案，所有文档需要存放在裁判组专门提供的U盘中。第三阶段是否提交文档，请根据现场具体题目要求。

选手首先需要在U盘的根目录下建立一个名为“xx工位”的文件夹，并在“xx工位”文件夹下，建立“第一阶段”、“第二阶段”两个文件夹，赛题两个阶段的文档分别归类放置在对应的文件夹中。

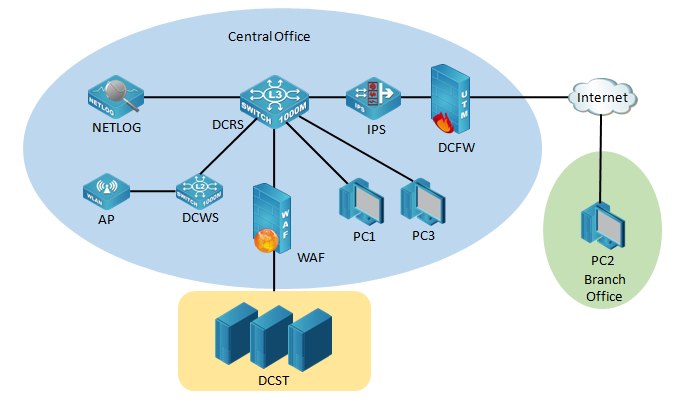
例如：08工位，则需要在U盘根目录下建立“08工位”文件夹，并在“08工位”文件夹下建立“第一阶段”、“第二阶段”两个文件夹。

特别说明：只允许在根目录下的“08工位”文件夹中体现一次工位信息，不允许在其他文件夹名称或文件名称中再次体现工位信息，否则按作弊处理。

赛项环境设置

赛项环境设置包含了三个竞赛阶段的基础信息：网络拓扑图、IP地址规划表、设备初始化信息。

1.网络拓扑图

PC环境说明：

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：Microsoft Internet Explorer 6.0

虚拟机安装服务/工具2：Ethereal 0.10.10.0

虚拟机安装服务/工具3：HttpWatch Professional Edition

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-2（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：Microsoft Internet Explorer 6.0

虚拟机安装服务/工具2：Ethereal 0.10.10.0

虚拟机安装服务/工具3：HttpWatch Professional Edition

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Kali Linux（Debian7 64Bit）

虚拟机安装服务/工具：Metasploit Framework

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

IP地址规划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **接口** | **IP地址** | **互联** | **可用IP数量** |
| 防火墙DCFW | EthX | x.x.x.x/x | 与PC-3相连 | 见赛场IP参数表 |
| EthX |  | 与IPS相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | SSL VPN地址池 | 见赛场IP参数表 |
| 入侵检测系统IPS | EthX |  | 与DCFW相连 | 见赛场IP参数表 |
| EthX |  | 与DCRS相连 | 见赛场IP参数表 |
| 无线交换机DCWS | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 地址池 | x.x.x.x/x | DCHP地址池 | 见赛场IP参数表 |
| WEB应用防火墙WAF | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| EthX |  | 与DCST相连 | 见赛场IP参数表 |
| 三层交换机DCRS | Vlan 2 | x.x.x.x/x | 与DCWS相连 | 见赛场IP参数表 |
| Vlan 10 | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| Vlan 20 | x.x.x.x/x | 与PC-1所在用户区相连 | 见赛场IP参数表 |
| Vlan 30 | x.x.x.x/x | 与PC-2所在用户区相连 | 见赛场IP参数表 |
| Vlan 40 | x.x.x.x/x | 与DCBI相连 | 见赛场IP参数表 |
| Vlan 100 | x.x.x.x/x | 直连服务器区 | 见赛场IP参数表 |
| Vlan 110 | x.x.x.x/x | 直连用户区 | 见赛场IP参数表 |
| Vlan 120 | x.x.x.x/x | 与IPS相连 | 见赛场IP参数表 |
| 网络日志系统DCBI | EthX | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 堡垒服务器DCST | EthX | x.x.x.x/x | 与WAF相连 | 见赛场IP参数表 |
| PC-1 | 无 | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| PC-2 | 无 | x.x.x.x/x | 与DCFW相连 | 见赛场IP参数表 |
| PC-3 | 无 | x.x.x.x/x | 与DCRS相连 | 见赛场IP参数表 |
| 服务器场景-1 | 无 | 见系统安全攻防加固赛题部分 | |  |
| 服务器场景-2 | 无 | 见系统安全攻防加固赛题部分 | |  |
| 服务器场景-3 | 无 | 见系统安全攻防加固赛题部分 | |  |
| 服务器场景-4 | 无 | 见系统安全攻防加固赛题部分 | |  |
| 服务器场景-5 | 无 | 见系统安全攻防加固赛题部分 | |  |
| 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。） | | | |

设备初始化信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备名称** | **管理地址** | **默认管理接口** | **用户名** | **密码** |
| 防火墙DCFW | <http://192.168.1.1> | ETH0 | admin | admin |
| 网络日志系统DCBI | https://192.168.5.254 | ETH0 | admin | 123456 |
| WEB应用防火墙WAF | https://192.168.45.1 | ETH5 | admin | admin123 |
| 入侵检测系统IPS | <http://192.168.1.1> | ETH0 | admin | admin |
| 三层交换机 | - | Console | - | - |
| 无线交换机DCWS | - | Console | - | - |
| 堡垒服务器DCST | http://192.168.1.100 | Eth0–Eth9 | 参见“DCST登录用户表” | |
| 备注 | 所有设备的默认管理接口、管理IP地址不允许修改;  如果修改对应设备的缺省管理IP及管理端口，涉及此设备的题目按 0 分处理。 | | | |

**第一阶段任务书（300分）**

该阶段需要提交配置或截图文档，命名如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **阶段** | **任务** | **序号** | **文档名称** |
| 第一阶段 | 任务1 | 1 | 任务1 |
| 2 | 赛场IP参数表 |
| 任务2 | 3 | 任务2-DCFW |
| 4 | 任务2-DCBI |
| 5 | 任务2-WAF |
| 6 | 任务2-IPS |
| 7 | 任务2-DCRS |
| 8 | 任务2-DCWS |

任务1：网络平台搭建（60分）

平台搭建要求如下：

|  |  |
| --- | --- |
| 题号 | 网络需求 |
| 1 | 根据网络拓扑图所示，按照IP地址参数表，对WAF的名称、各接口IP地址进行配置。 |
| 2 | 根据网络拓扑图所示，按照IP地址参数表，对DCRS的名称、各接口IP地址进行配置。 |
| 3 | 根据网络拓扑图所示，按照IP地址参数表，对DCFW的名称、各接口IP地址进行配置。 |
| 4 | 根据网络拓扑图所示，按照IP地址参数表，对DCWS的各接口IP地址进行配置。 |
| 5 | 根据网络拓扑图所示，按照IP地址参数表，对DCBI的名称、各接口IP地址进行配置。 |
| 6 | 根据网络拓扑图所示，按照IP地址参数表，对IPS的名称、各接口IP地址进行配置。 |
| 7 | 根据网络拓扑图所示，按照IP地址参数表，在DCRS交换机上创建相应的VLAN，并将相应接口划入VLAN。 |
| 8 | 采用静态路由的方式，全网络互连。 |
| 9 | 完整填写“赛场IP参数表”。 |

任务2：网络安全设备配置与防护（240分）

DCFW:

1. 在总公司的DCFW上配置，连接LAN接口开启PING,HTTP,HTTPS功能，连接Internet接口开启PING、HTTPS功能；并且新增一个用户，用户名dcn2017，密码dcn2017，该用户只有读-执行权限；
2. DCFW连接LAN的接口配置二层防护，ARP Flood超过500个每秒时丢弃超出的ARP包，ARP扫描攻击超过300个每秒时弃超出的ARP包；配置静态ARP绑定，MAC地址880B.0A0B.0C0D与IP地址X.X.X.X绑定；
3. DCFW连接Internet的区域上配置以下攻击防护：

FW1，FW2攻击防护

启以下Flood防护：

ICMP洪水攻击防护，警戒值2000，动作丢弃；

UDP供水攻击防护，警戒值1500，动作丢弃；

SYN洪水攻击防护，警戒值5000，动作丢弃；

开启以下DOS防护：

Ping of Death攻击防护；

Teardrop攻击防护；

IP选项，动作丢弃；

ICMP大包攻击防护，警戒值2048，动作丢弃；

1. DCFW上配置NAT功能，使PC2能够通过WEB方式正常管理到WAF，端口号使用10666;）
2. 总公司DCFW配置SSLVPN，建立用户dcn01，密码dcn01，要求连接Internet PC2可以拨入，配置下载客户端端口为9999，数据连接端口为9998，SSLVPN地址池参见地址表；
3. DCFW上配置ZONE和放行策略，连接Internet接口为“Untrust”区域，连接DCRS接口为“Trust”区域，连接SSL VPN接口为“VPN HUB”区域，要求配置相应的最严格安全策略；）

IPS:

1. IPS串联在DCFW与DCRS中间进行威胁检测与防御，配置IPS为透明模式，根据题意配置“Trust”区域与“Untrust”区域，并配置相应的放行策略；
2. 配置入侵检测特征模板如下：针对Windows系统Samba协议的缓冲区溢出攻击，如流量匹配此模板则阻止流量并发送告警信息；
3. 配置病毒检测，对于来自Internet的通过HTTP、FTP、POP3协议所接收的压缩文件RAR、ZIP进行病毒检测，并阻止携带病毒的压缩文件流入内网；

DCBI:

1. 在公司总部的DCBI上配置，设备部署方式为旁路模式，并配置监控接口与管理接口;增加非admin账户DCN2017，密码dcn2017，该账户仅用于用户查询设备的系统状态和统计报表;
2. 在公司总部的DCBI上配置，监控周一至周五9：00-18：00 PC-1所在网段用户访问的URL中包含xunlei的HTTP访问记录，并且邮件发送告警;
3. 在公司总部的DCBI上配置，监控PC-1所在网段用户周一至周五9：00-18：00的即时聊天记录;
4. 公司总部LAN中用户访问网页中带有“MP3”、“MKV”、“RMVB”需要被DCBI记录；邮件内容中带有“银行账号”记录并发送邮件告警；
5. DCBI监控LAN中用户访问网络游戏，包括“QQ游戏”、“魔兽世界”并作记录；
6. DCBI配置应用及应用组“快播视频”，UDP协议端口号范围23456-23654，在周一至周五9：00-18：00监控LAN中所有用户的“快播视频”访问记录；
7. DCBI上开启邮件告警，邮件服务器地址为X.X.X.X，端口号25,告警所用邮箱用户名dcnadmin,密码Dcn2017;当DCBI磁盘使用率超过75%时发送一次报警；

WAF:

1. 在公司总部的WAF上配置，编辑防护策略，定义HTTP请求体的最大长度为512，防止缓冲区溢出攻击；
2. 在公司总部的WAF上配置，防止某源IP地址在短时间内发送大量的恶意请求，影响公司网站正常服务。大量请求的确认值是：10秒钟超过3000次请求；
3. 在公司总部的WAF上配置，对公司网站（X.X.X.X）进行安全评估，检查网站是否存在安全漏洞，便于在攻击没有发生的情况下提前做出防护措施；
4. 使用WAF自带标识组配置爬虫防护与扫描防护，阻断时间120秒，通过WAF组织爬虫探测和扫描服务器区域；
5. 在公司总部的WAF上配置，禁止HTTP请求和应答中包含敏感字段“赛题”和“答案”的报文经过WAF设备。
6. 公司web应用防火墙透明模式部署，为了防止不法人员对公司内的网站(X.X.X.X)进行攻击，在web 应用防火墙上开启“黑名单”策略，禁止公网IP地址（X.X.X.X）访问网站服务器。
7. 公司web应用防火墙透明模式部署，为了防止不法人员对公司内的网站(X.X.X.X)进行攻击，在web 应用防火墙上开启防止“SQL注入”攻击策略阻止攻击流量；
8. 在公司总部的WAF上配置， WAF设备的内存使用率超过75%每隔5分钟发送邮件和短信给管理，邮箱[admin@digitalchina.com](mailto:admin@digitalchina.com)，手机13912345678；

DCRS:

1. DCRS为接入交换机，为终端产生防止MAC地址防洪攻击，请配置端口安全，每个已划分VLAN的端口最多学习到5个MAC地址，发生违规阻止后续违规流量通过，不影响已有流量并产生LOG日志；Ex/x为专用接口，限定MAC地址00-11-11-11-11-11可以连接；将连接DCFW的双向流量镜像至Netlog进行监控和分析；
2. DCRS配置802.1x认证，Radius服务器IP 地址X.X.X.X,认证密码Dcn2017,
3. Ex/x号端口开启802.1x功能，接入该端口通过PC上的802.1x软件进行认证；
4. 接入DCRS Ex/x，仅允许IP地址X.X.X.X-X.X.X.X为源的数据包为合法包，以其它IP地址为源地址，交换机直接丢弃；
5. 为拦截，防止非法的MAC地址与IP地址绑定的ARP数据包，配置动态ARP检测功能，AC为DHCP服务器，限制与AC在同一VLAN接口的ARP阀值为50；
6. DCRS上开启以下安全特性，防IP Spoofing攻击、防TCP非法标志攻击、防端口欺骗攻击、防TCP碎片攻击、防ICMP碎片攻击；

DCWS:

1. AP通过option43方式进行正常注册上线；
2. 设置AP工作在5G频段；
3. 设置SSID DCN，加密模式为wpa-personal,其口令为：chinaskill；

设置SSID GUEST 不进行认证加密；

1. GUSET最多接入10个用户，用户间相互隔离，并对GUEST网络进行流控，上行1M，下行2M；
2. 通过配置避免接入终端较多且有大量弱终端时，避免高速客户端被低速客户端“拖累”，让低速客户端不至于长时间得不到传输；
3. 通过使用黑名单技术禁止mac地址为68-a3-c4-e6-a1-be的PC通过无线网络上网；
4. 防止非法AP假冒合法SSID，开启AP威胁检测功能；
5. 通过设置实现在AC断开网络连接时AP还能正常工作；
6. 考虑到无线网络会进一步部署，增加更多的AP，设置已有AP信道和发射功率每隔1小时自动调节；
7. 为防止增多AP后产生过多的ARP数据包，开启ARP抑制功能，要求AC能代为应答其已知的MAC地址；

**第二阶段任务书（400分）**

提示：本阶段用到堡垒服务器DCST中的服务器场景，获取服务器IP地址方式如下：

Windows服务器的IP地址可以通过拓扑界面获得，如果获得不了，采用如下方法获得：

通过DCST场景里的网络拓扑图，启动连接设备

进入服务器，用户名为administrator，密码：空

执行ipconfig /all，即可获得服务器IP地址

任务1：缓冲区溢出漏洞渗透测试

任务描述：

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中某程序可能存在缓冲区溢出漏洞；你需要对该程序进行渗透测试，确认程序确实存在该漏洞；

任务环境说明：

主机场景：WindowsXP

主机场景操作系统：Microsoft Windows XP Professional

主机场景安装服务/工具1：Visual C++ 6.0；

主机场景安装服务/工具2：OllyICE；

主机场景安装服务/工具3：Findjmp；

主机场景安装服务/工具4：Sublime Text 2.0.2；

任务内容：

1. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行分析，找到Main函数中有缓冲区溢出可能的变量名，并将Flag值（形式：有缓冲区溢出可能的变量名）进行提交；
2. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，使用工具findjmp找到Windows内核文件KERNEL32.DLL中的首个“call esp”指令的内存地址，将该内存地址作为函数的返回地址，根据以上信息，填写可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）中的F1字符串，并将Flag值（形式：F1字符串内容）进行提交；
3. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中join函数中的F2、F3字符串，并将Flag值（形式：F2字符串内容;F3字符串内容）进行提交；
4. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中repstr函数中的F4、F5字符串，并将Flag值（形式：F4字符串内容;F5字符串内容）进行提交；
5. 对可能存在缓冲区溢出的程序源代码（位置：C:\VC\Source Code\Overflow.c）进行完善，填写该源代码中main函数中的F6、F7、F8字符串，并将Flag值（形式：F6字符串内容;F7字符串内容;F8字符串内容）进行提交；
6. 将完善后的缓冲区溢出渗透测试程序源代码（位置：C:\VC\Source Code\Overflow.c）进行编译、链接、运行，将该程序的运行结果显示的最后1行字符串作为Flag值（形式：程序的运行结果显示的最后1行字符串）提交；

任务2：Web应用程序安全攻防

任务描述：

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中Web应用程序可能存在SQL注入漏洞；首先，你需要对该程序进行渗透测试，确认程序确实存在该漏洞；其次，你需要对该程序打补丁，解决以上漏洞带来的问题；第三，你需要再次对该程序进行渗透测试，验证程序是否还存在漏洞。

任务环境说明：

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：Microsoft Internet Explorer 6.0

虚拟机安装服务/工具2：Ethereal 0.10.10.0

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

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. 在PC-1上，Web访问DCST中的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，并将所有提交的变量名作为Flag值（形式：变量名1;变量名2;…;变量名n）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站点可通过万能用户名、数据库users表中当中任意一个密码登录，并将万能用户名字符串当中的固定部分作为Flag值（形式：万能用户名字符串当中的固定部分）提交；
3. 对服务器场景：WebServ2003的Web开发环境进行配置，使其能够支持数据抽象层（PDO）技术，并将配置文件的路径及名称字符串作为Flag值（形式：配置文件的路径及名称字符串）提交；
4. 对服务器场景：WebServ2003的Web开发环境进行配置，使其能够支持数据抽象层技术，并将在上题配置文件中取消注释行内容作为Flag值（形式：按顺序取消注释行1字符串; 按顺序取消注释行1字符串;…; 按顺序取消注释行n字符串）提交；
5. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；
6. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；
7. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；
8. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；
9. 进入DCST中的WebServ2003服务器场景目录，找到login.php页面参数提交到的php文件，分析并使用EditPlus工具修改该php源程序，使之可以抵御SQL注入渗透测试，并填写该php源程序当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；
10. 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该DCST中的WebServ2003服务器场景进行SQL注入渗透测试无效，并将页面回显HTML源文件内容作为Flag值（形式：页面回显HTML源文件内容）提交；

任务3：ARP扫描渗透测试

任务描述：

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，现欲对该系统中主机进行ARP扫描渗透测试，确认该系统中都有哪些IP主机在线；

任务环境说明：

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：CentOS5.5

服务器场景操作系统：CentOS Linux 5.5

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_sweep.py文件，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；（arp\_sweep.py脚本功能见该任务第6题）
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arp\_sweep.py文件，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；（arp\_sweep.py脚本功能见该任务第6题）
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arp\_sweep.py文件，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；（arp\_sweep.py脚本功能见该任务第6题）
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arp\_sweep.py文件，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；（arp\_sweep.py脚本功能见该任务第6题）
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arp\_sweep.py文件，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；（arp\_sweep.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行arp\_sweep.py文件，对服务器场景进行ARP扫描渗透测试；将该文件执行后的显示结果中，第1行的第1个字符以及第2行的第1个字符作为Flag值（形式：第1行的第1个字符;第2行的第1个字符）提交；

任务4：操作系统判断渗透测试

任务描述：

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，现欲对该系统中主机进行操作系统扫描渗透测试，确认该系统中主机都运行了哪些操作系统；

任务环境说明：

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

服务器场景：CentOS5.5

服务器场景操作系统：CentOS Linux 5.5

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的os\_scan.py文件，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；（os\_scan.py脚本功能见该任务第6题）
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os\_scan.py文件，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；（os\_scan.py脚本功能见该任务第6题）
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os\_scan.py文件，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；（os\_scan.py脚本功能见该任务第6题）
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os\_scan.py文件，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；（os\_scan.py脚本功能见该任务第6题）
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os\_scan.py文件，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；（os\_scan.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行os\_scan.py文件，对服务器场景进行操作系统信息判断渗透测试，将该文件执行后的显示结果作为Flag值（形式：文件执行后的显示结果字符串）提交；

任务5：数据库访问渗透测试及其加固

任务描述：

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中Web服务器中的数据库服务可能存在访问漏洞；首先，你需要对该程序进行渗透测试，确认程序确实存在该漏洞；其次，你需要对数据库服务进行安全加固配置，解决以上漏洞带来的问题；第三，你需要再次对该程序进行渗透测试，验证程序是否还存在访问漏洞。

任务环境说明：

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

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. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mssql\_brute\_force.py文件，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；（mssql\_brute\_force.py脚本功能见该任务第6题）
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mssql\_brute\_force.py文件，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；（mssql\_brute\_force.py脚本功能见该任务第6题）
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mssql\_brute\_force.py文件，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；（mssql\_brute\_force.py脚本功能见该任务第6题）
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mssql\_brute\_force.py文件，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；（mssql\_brute\_force.py脚本功能见该任务第6题）
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mssql\_brute\_force.py文件，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；（mssql\_brute\_force.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行mssql\_brute\_force.py文件，进行数据库超级管理员密码暴力破解渗透测试（使用字典文件./root/superdic.txt），将该文件执行后的显示结果中的最后1行内容作为Flag值（形式：文件执行后的显示结果中的最后1行字符串）提交；
7. 通过对服务器场景WebServ2003的数据库服务进行安全加固，阻止PC-3中渗透测试平台对其进行数据库超级管理员密码暴力破解渗透测试，并将进行安全配置的数据库身份验证选项中的英文单词作为Flag值（形式：进行安全配置的数据库身份验证选项中的唯一一个英文单词字符串）提交；
8. 验证在WebServ2003的数据库服务进行安全加固后，再次在虚拟机操作系统：Ubuntu Linux 32bit下执行mssql\_brute\_force.py文件，进行数据库超级管理员密码暴力破解渗透测试（使用字典文件./root/superdic.txt），将该文件执行后的显示结果中的最后1行内容作为Flag值（形式：文件执行后的显示结果中的最后1行字符串）提交；

任务6：网络协议渗透测试及其加固

任务描述：

假定各位选手是TaoJin电子商务企业的信息系统安全工程师，负责该企业信息系统的安全维护，在该系统中的网络通讯协议可能存在漏洞；首先，你需要对网络进行渗透测试，确认网络协议确实存在该漏洞；其次，你需要对网络通讯协议进行安全加固配置，解决以上漏洞带来的问题；第三，你需要再次对该网络进行渗透测试，验证网络是否还存在访问漏洞。

任务环境说明：

PC-1（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：WindowsXP

虚拟机安装服务/工具1：EditPlus

虚拟机安装服务/工具2：XFTP

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

PC-3（须使用物理机中的虚拟机）：

物理机操作系统：Windows7 64位旗舰版

VMware Workstation 12 Pro

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具集：BackTrack5

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

DCST：

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. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的mac\_flood.py文件，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；（mac\_flood.py脚本功能见该任务第6题）
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mac\_flood.py文件，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；（mac\_flood.py脚本功能见该任务第6题）
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mac\_flood.py文件，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；（mac\_flood.py脚本功能见该任务第6题）
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mac\_flood.py文件，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；（mac\_flood.py脚本功能见该任务第6题）
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mac\_flood.py文件，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；（mac\_flood.py脚本功能见该任务第6题）
6. 在虚拟机操作系统：Ubuntu Linux 32bit下执行mac\_flood.py文件，进行MAC Flooding渗透测试；运行DCRS交换机命令（#show mac-address-table count），将该命令执行结果显示的交换机学习到的当前动态MAC地址条目总数作为Flag值（形式：动态MAC地址条目总数）提交；
7. 在DCRS交换机的PC-3所连接端口配置端口安全特性，阻止PC-3发起MAC Flooding渗透测试，将配置的端口模式配置命令字符串作为Flag值（形式：端口模式配置命令字符串）提交；
8. 再次在虚拟机操作系统：Ubuntu Linux 32bit下执行mac\_flood.py文件，进行MAC Flooding渗透测试；运行DCRS交换机命令（#show mac-address-table count），将该命令执行结果显示的交换机学习到的当前动态MAC地址条目总数作为Flag值（形式：动态MAC地址条目总数）提交；

**第三阶段任务书（300分）**

假定各位选手是Taojin电子商务企业的信息安全工程师，负责服务器的维护，该服务器可能存在着各种问题和漏洞（见以下漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多白帽黑客（其它参赛队选手）对这台服务器进行渗透测试。

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：任何时候不能人为关闭服务器服务端口，否则将判令停止比赛，第三阶段分数为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，第三阶段分数为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，第三阶段分数为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。

注意5：靶机的Flag值存放在./root/flaginfoxxxx.xxx.txt文件内容当中。

注意6：每提交1次对手靶机的Flag值增加4分，每当被对手提交1次自身靶机的Flag值扣除4分，每个对手靶机的Flag值只能提交一次。

注意7：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。

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。

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。

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）

**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

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三个方面的能力和水平。

1．按照要求正确连接并配置网络、服务器、虚拟化设备和安全设备等，构建信息系统。

2．按照要求进行信息系统风险评估（单兵作战），并对信息系统进行加固，形成完整信息系统的风险评估和安全加固方案。

3．按照要求对其他组的信息系统进行渗透（分组对抗模式）。

（二）评分方法

比赛过程中参赛队第二阶段和第三阶段的得分情况由系统自动统计，由裁判委员会统一评定；

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，不计参赛选手个人得分；

在竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为的，由裁判长按照规定扣减相应分数，情节严重的取消比赛资格，比赛成绩记0分；

竞赛评分细则按照本竞赛规程在竞赛开始7天之前由执行委员会制定。

（三）评分细则

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **竞赛阶段** | **竞赛任务** | **考核内容** | **分值** | **评分方式** |
| 第一阶段  权重30% | 网络平台搭建  权重9% | 网络规划文档 | 2% | 结果评分-客观 |
| 网络设备配置文件或截图文件 | 7% | 结果评分-客观 |
| 网络安全设备配置与防护  权重21% | 防火墙配置截图文件 | 21% | 结果评分-客观 |
| 网络日志系统配置截图文件 | 结果评分-客观 |
| 入侵检测系统配置截图文件 | 结果评分-客观 |
| web应用防火墙配置截图文件 | 结果评分-客观 |
| 无线控制器配置文件 | 结果评分-客观 |
| 三层交换机配置文件 | 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 |
| 第三阶段  权重30% | 分组对抗  权重30% | 防守成功，坚持到竞赛结束 | 10% | 机考评分 |
| 渗透成功（每渗透成功1队得2分） | 20% | 机考评分 |

**十一、奖项设置**

竞赛奖项只设置团体奖，团体奖根据参赛代表队总得分，进行排序（总分相同名次并列）。设一等奖10%，二等奖20%，三等奖30%。

**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》 |
| 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 |

**十三、建议使用的比赛器材、技术平台和场地要求**

（一）网络设备竞赛器材（硬件平台）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **参数** |
| 1 | 三层虚拟化交换机 | 1 | 24个千兆以太网电口+4个复用千兆SFP光口+4个10G SFP+光口，支持双热插拔AC & DC电源。 |
| 2 | 防火墙 | 1 | 9个10/100/1000M以太网电口；1U标准机箱。 |
| 3 | 堡垒服务器 | 1 | 平台内置WINDOWS、LINUX系统管理、数据恢复等课程，同时内置安全扫描、病毒、木马等诸多课程。 |
| 4 | WEB应用防火墙 | 1 | 对HTTP协议进行深入分析，为Web应用提供全面的实时有效的防御能力，解决Web应用安全问题，优化业务资源，采用1U标准机箱，内置6个10/100/1000以太网电口。 |
| 5 | 入侵检测系统 | 1 | 支持基于IP碎片重组、TCP流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别； 支持模式匹配、异常检测、统计分析，以及抗IDS/IPS逃逸等多种检测技术。 |
| 6 | 网络日志系统 | 1 | 采用1U机架式，6个千兆电口，可实现网站访问、BBS/留言、网络游戏、下载、各种股票流量、即时消息、邮件等的分析记录与控制管理。 |
| 7 | 无线交换机 | 1 | 有线无线一体化智能控制器，4个千兆SFP光口，24个千兆PoE电口，全部电口支持最大30W （802.3at标准）供电，最大PoE供电功率370W。 |
| 8 | 无线接入点 | 1 | 室内802.11ac放装式无线AP，内置天线，2.4G/5G双频，整机4条空间流，整机最大速率1.167Gbps，支持802.11a/n/ac和802.11b/g/n同时工作，1个千兆口+1个百兆口，支持USB 2.0口。 |
| 9 | 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。 |

（二）软件技术平台：

比赛的应用系统环境主要基于桌面版和服务器版组成，桌面版主要采用Windows XP Pro (中文版)和Windows 7 (中文版)两个版本，服务器版本根据需要以windows和linux系统为主，版本涉及各类版本；办公软件主要为Microsoft Office 2007(中文版)、RAR 4.0 (中文版)、Adobe Reader阅读器；比赛提供sercureCRT7.0作为终端。

具体软件参数如下表所示：

1．微软 Windows XP Pro (中文版) 30天试用版

2．微软 Windows 7 (中文版) 30天试用版

3．RAR 4.0 (中文版) 免费版

4．微软 Microsoft Office 2007(中文版) 30天试用版

5．SercureCRT 7.0绿色版

6．Adobe Reader阅读器（中文版）免费版

（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，具备至少安排80支参赛队的竞赛场地。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带点车辆、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**

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。

（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，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。

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。

参赛队：由各省市负责参赛选手旅途及竞赛过程中的安全保障。

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，也可进行赛场环境还原测试，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。

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）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. 大赛期间有组织的参观和观摩活动的交通安全由赛区组委会负责。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，除了可以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。

（五）组队责任

1. 各省、自治区、直辖市和计划单列市在组织参赛队时，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。

3. 各参赛队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。

（六）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。

（七）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. 因参赛队伍原因造成重大安全事故的，取消其参赛资格。

3. 参赛队伍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。

**十五、经费概算**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **费用类别** | | **项目** | **金额（元）** | **备注** |
| 预算收入 | | 企业赞助 | 600000 | 赛项赞助企业承诺支持 |
| 预算支出 | | 研讨论证会 | 80000 | 研讨会专家的用餐、住宿等 |
| 竞赛试题开发 | 40000 | 专家封闭开发住宿、用餐等费用 |
| 印刷费 | 20000 | 大赛通知、赛程、竞赛文档、赛题等 |
| 裁判培训费 | 20000 | 裁判员培训费用 |
| 场地布线和布置 | 100000 | 根据比赛要求布置场地 |
| 赛项器材的使用费 | 50000 | 赛事器材的运输、安装、布置、调试费用 |
| 赛项比赛耗材费 | 10000 | 耗材费用（纸、墨盒、网线等） |
| 赛项专家工作费 | 24000 | 按照10名专家计算 |
| 赛项裁判费 | 45000 | 按照30名裁判计算 |
| 现场技术支持 | 20000 | 竞赛现场支持 |
| 赛项内场宣传费 | 45000 | 宣传材料制作， 媒体网站维护等 |
| 工作人员餐费 | 10000 | 比赛当天工作人员两顿正餐用餐 |
| 参赛队伍餐费 | 10000 | 比赛当天参赛队伍午餐用餐 |
| 赛项参赛服装费 | 20000 | 选手、裁判、指导教师、领队、技术支持统一服装 |
| 赛项获奖选手奖品费 | 36000 | 获奖选手一二三等奖品 |
| 赛项摄录像与资源转化费 | 40000 | 赛事期间资料保存和赛后资源转化 |
| 赛项经费统筹支出及其他费用 | 30000 |  |
|  | **支出合计（元）** | | **600000** |  |

**十六、比赛组织与管理**

（一）设立赛项执行委员会，负责整个比赛的组织与管理。

（二）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。

（三）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。

（四）设立仲裁组：组长一名、组员若干，负责赛项的仲裁工作。

（五）下设立裁判组：裁判长一名、裁判若干，负责赛项的裁判工作。

（六）设现场赛务组：组长一名，组员若干，负责赛场场地内设备及人员管理。

（七）安保组：组长一名，组员若干，负责赛场及周边的安保工作。

（八）秘书组：组长一名，组员若干，负责撰文等文案工作。

（九）宣传组：组长一名，组员若干，负责赛项宣传等联系工作。

（十）设计组：组长一名，组员若干，负责赛项场地、布展等工作。

（十一）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**

依照《2017年全国职业院校技能大赛赛项资源转化工作办法》的有关要求，赛后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。

第一类资源转化的内容是赛项竞赛全过程的各类资源，包括：

（一）竞赛样题、试题库。

（二）竞赛技能考核评分案例。

（三）考核环境描述。

（四）竞赛过程音视频记录。

（五）评委、裁判、专家点评。

（六）优秀选手、指导教师访谈。

第二类资源转化的内容：课程建设

从2011年开始，在大赛赛后，专家组都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。

本赛项赛2016年出版3本教材，《网络安全项目实践》、《信息系统安全项目实战》、《网络信息安全实践习题与解答》3本教材可以作为信息安全和网络技术专业补充教学资源使用；2017年与院校合作编写1本教材《信息安全基础》，该教材是普适性安全教材适用于高职院校所有专业的公共基础课，可以提升非电子信息类学生的信息安全水平

第三类资源转化内容：交互微课建设以及微课平台建设

专业建设在内涵建设工程中具有不可替代的基础性地位，它是职业院校各项建设工作的重中之重，这是由职业院校的社会职能和办学目标所决定的。在《关于实施国家中等职业教育改革发展示范学校建设计划的意见》中明确提出了“以适应职业岗位需求为导向，加强实践教学”、“通过数字技术、还原现实等信息化方式，在教学中普遍应用现代信息技术，多渠道系统优化教学过程，增强教学的实践性、针对性和实效性，提高教学质量”等要求。

开发在线交互式实训课件开发工具进行微课建设，将多媒体技术、应用场景还原技术以及人机交互技术有机结合在一起，赛后计划开发30个信息安全比赛的训练课件。目前已经搭建了微课平台，开放了30个免费使用的帐号，为职业院校师生提供课件教学服务。

第四类资源转化内容：师资队伍建设

2018年大赛完毕后计划进行2期研讨会，以及5期师资培训,培训内容定为信息安全在工作与生活中的应用，系统信息安全实战，网络信息安全实战，数据安全及取证技术，数据中心灾备技术、无线网络安全等内容。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **活动名称** | **计划时间** | **备注** |
| 1 | 研讨会第1期 | 2018年7月 |  |
| 2 | 师资培训第1期 | 2018年7月 |  |
| 3 | 师资培训第2期 | 2018年7月 |  |
| 4 | 师资培训第3期 | 2018年8月 |  |
| 5 | 师资培训第4期 | 2018年8月 |  |
| 6 | 师资培训第5期 | 2018年9月 |  |
| 7 | 研讨会第2期 | 2018年10月 |  |

**十八、筹备工作进度时间表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **筹备阶段** | **内　容** | **时间安排** |
| 1 | 申报、立项 | 赛项设计专家研讨会，完成赛项申报方案 | 2017年9月 |
| 确定赛项 | 2017年11月 |
| 成立赛项执委会、专家组 |
| 2 | 赛前准备 | 赛项专家会议3-5轮次会议，确定赛项规程、样题、赛项技术方案、赛场方案、体验环节设计方案、开放方案、宣传方案、教学资源转化方案、赛事安全规章、突发事件应急预案等 | 2017年11月～2018年1月 |
| 确定分赛区及承办校 | 2018年2月 |
| 全国赛项说明会 | 2018年4月 |
| 命题专家组会议，赛题开发、确定竞赛题库 | 2018年4月 |
| 赛项预报名及报名完成 | 2018年4月 |
| 3 | 比赛阶段 | 比赛设备安装、调试，赛场布置、同期技术展示、体验和活动现场布置；赛项指南印刷、选手服装制作 | 2018年5月 |
| 专家组题库审核，确定评分标准及抽题 |
| 成立裁判组、仲裁组、监督组；培训并验收赛场 |
| 正式比赛、同期技术展示、体验和活动举办；竞赛成绩提交、竞赛过程文档提交、教学资源转化成果与赛项总结 |

**十九、裁判人员建议**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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，熟悉信息安全类别和主要攻防手段 | 具有相关专业教学工作经验或电子信息类省级或国家级执裁经验 | 工程师、高级工程师、副教授、教授 | 10 |
| 2 | 信息安全、计算机网络方向 | 熟悉网络基础以及windows和linux操作系统，熟悉系统加固及安全评估流程，熟悉信息安全主要类别和主要攻防手段，熟练调试主流网络设备 | 具有相关专业教学工作经验或电子信息类省级或国家级执裁经验 | 工程师、高级工程师、副教授、教授 | 10 |
| **裁判总人数** | 20 | | | | |

**二十、其他**

该赛项为2011年-2017年连续举办六年的国赛项目，历届比赛都圆满成功，得到了相关领导及各参赛队的高度评价。赛项规模也不断扩大，起到了很好的引领作用。

承诺并保证开赛一个月前在大赛网络信息发布平台（www.chinasklls-jsw.org）公开全部赛题。