**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

信息安全管理与评估

（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** | **专业大类** | **专业类** | **专业代码** | **专业名称** |
| 高职 | 电子信息 | 计算机 | 610211 | 信息安全与管理 |

##### 赛项申报专家组

##### 三、赛项目的

（一）检验教学成果

本赛项旨在考察参赛选手在企业真实项目环境下安全网络搭建、按照等保要求加固网络、安全架构、渗透测试、攻防实战等信息安全领域的核心技术能力，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。通过竞赛激发学生学习的热情和参与企业工程项目的积极性，实现“以赛促学”，达到培养更多符合企业岗位实际需求的高技术技能人才的目的；

（二）强化专业建设

针对国家“十三五”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》的信息安全与管理专业建设标准，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”等专业核心课程内容。

（三）促进产教合作

赛项设计紧密结合产业发展对人才需求的标准，内容基于信息安全领域主流技术和现行业务流程设计。通过信息安全行业专家与院校教育专家紧密合作，搭建校企合作平台，深化产教融合。赛后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清单和设备技术文档，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进行针对竞赛内容的集训，提高专业水平；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，竞赛的试题内容与真实工程实践相符合，既充分考核了学生解决问题的综合能力，也考核了学生工程实践能力。通过赛题公开的形式保证了竞赛的公平性。。

（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

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，全国高职院校开设信息安全与管理专业和网络技术的院校已经超过1000多所，专业覆盖率超过75%，在校生超过40多万。

赛项设计符合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，符合国家信息产业发展要求。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。

根据国家十三五规划纲要，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，因此将无线网络安全等相关技术加入到赛项中，包括无线网络搭建，支持IEEE 802.11n最新的无线高速接入技术， WEP和WPA认证，MAC地址准入控制等的多种无线网络安全技术。

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，2019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。

（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

赛项内容高度覆盖了信息安全与管理专业、计算机网络专业等相关专业职业岗位群技能要求，与信息安全技术支持、网络安全运维、网络安全测评、信息安全产品销售、网络工程搭建等职业岗位人才技能培养吻合度高，竞赛内容体现了对学生安全网络搭建、系统加固、安全系统评估、无线网络安全、Web安全攻防等专业核心能力的培养，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）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

采用的设备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，该赛项办赛时间长，技术成熟，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）竞赛方案强调协同性

赛项方案强调多个协同：一是竞赛选手之间相互协同。使选手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”与以学生为主动的“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）加入自动评分功能，使比赛结果更加公平

自2017年开始赛项专门设计了竞赛自动评分系统，70%的比赛计分采用计算机系统自动评分模式，保障大赛计分的准确性、实时性、公平性，并且可以做到与场外大屏实时互动，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）竞赛过程具备趣味性和观赏性

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）以赛促改，推进竞赛成果向教学资源转化。

2018年信息安全管理与评估竞赛项目已进行了教学成果的转化，设计了基于竞赛的生产性实训项目，完成了竞赛过程的网页课件的开发，开发了基于竞赛的规划教材，2019年将继续完成竞赛成果的教学资源转化，并进一步开发交互式实训用于辅助教学，促进专业教学资源的建设。

（五）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《2018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，针对信息安全与管理专业学生的“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、按照等保要求进行安全加固的能力，职业道德、组织管理能力、工作计划性和团队协作精神相关职业素养，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。

竞赛内容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 Information Security 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, Capacity for safety reinforcement in accordance with equal warranty requirements,professional ethics,management of organizing, working arrangement and the spirit of teamwork related professionalism,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2019年在籍的高职学生，性别不限，年龄不超过25周岁。

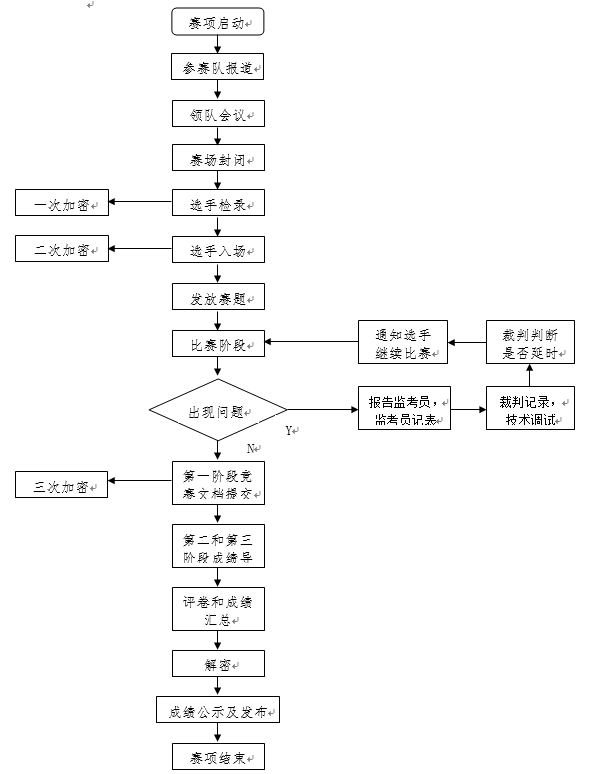
（二）竞赛分预赛和决赛两个阶段。

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2019年全国职业院校技能大赛组委会统一组织。

（三）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，宣读考场纪律和赛题发放时间 |
| 09:00-13:30 | 第一阶段和第二阶段正式比赛时间 |
| 13:30-14:00 | 第一阶段比赛结果提交时间，三次加密 |
| 14:00-15:00 | 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

本赛项已建立试题库，试题库中共有10套题目。

竞赛样卷请见附件1。

##### 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  依据评价标准验证结果正确性 |
| 按照等保要求进行网络设备配置,提交配置文件和截图文件 | 7% | 结果评分-客观  依据评价标准验证结果正确性 |
| 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  依据评价标准验证结果正确性 |
| 网络日志系统配置截图文件 | 结果评分-客观  依据评价标准验证结果正确性 |
| web应用防火墙配置截图文件 | 结果评分-客观  依据评价标准验证结果正确性 |
| 无线控制器配置文件 | 结果评分-客观  依据评价标准验证结果正确性 |
| 三层交换机配置文件 | 结果评分-客观  依据评价标准验证结果正确性 |
| 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  依据Flag值验证结果的正确性 |
| 服务器渗透配置 | 20% | 机考评分  依据Flag值验证结果的正确性 |
| 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  依据Flag值验证结果的正确性 |
| 渗透成功，获得相应分数 | 20% | 机考评分  依据Flag值验证结果的正确性 |

##### 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 |
| 15 | BG/T 22239-2008 | 信息安全技术信息系统安全等级保护基本要求 |

##### 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。 |
| 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 | 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。 |
| 6 | 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。 |
| 7 | 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，支持USB 2.0口。 |
| 8 | 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100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 | 35000 | 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 | 26000 | 获奖选手一二三等奖品 |
| 赛项摄录像、照像、宣传与资源转化费 | 60000 | 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《2018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基本资源，包括：

（一）风采展示

赛项宣传片和获奖代表队风采展示片。

（二）技能概要

技能介绍、技能操作要点、评价指标。

（三）教学资源

为更好地发挥信息安全管理与评估赛项对信息安全与管理及相关专业的教学改革与专业发展的引领作用，突出大赛对技术技能人才培养的作用，2018年竞赛结束后，联合参赛院校与合作企业成立了资源转化工作组，开展基于课程资源建设、师资培训等一系列资源转化的活动，目前完成了一整套教材资源内容：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。编写并出版了《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》、《信息安全基础》4本教材，开发信息安全项目综合实训案例1套，组织了8次师资培训，同时推出信息安全认证课程及考试，认证课程内容与国赛内容接轨，既可以用于教师技能再提升，也可以用于信息安全课程置换，通过认证课程及考试进一步完善大赛资源转化成果与信息安全专业建设。

第二类资源转化的内容是拓展资源。

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。

资源转化项目工作进程表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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本 | 电子教材 | 赛后90日 | 专家组  技术支持单位 |
| 拓 展 资 源 | 案例集 | | 文本 | 1套 | 教材、文档、图片、视频等，  补充完善 | 赛后90日 | 专家组  技术支持单位 |
| 仿真微课 | | 资源库 | 1套 | 云微课平台  补充完善 | 赛后90日 | 专家组  技术支持单位 |
| 优秀选手访谈 | | 视频 | 1 | 结合19年比赛补充完善 | 赛后90日 | 承办校 |

##### 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 | 2018年9月 |
| 确定赛项 | 2018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 | 2018年11月～2019年1月 |
| 确定分赛区及承办校 | 2019年2月 |
| 全国赛项说明会 | 2019年4月 |
| 命题专家组会议，赛题开发、确定竞赛题库 | 2019年4月 |
| 赛项预报名及报名完成 | 2019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 | 2019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

赛项所需现场裁判和评分裁判在能遵守《全国职业院校技能大赛专家和裁判工作管理办法》的前提下，参照有关要求，竞赛裁判组由裁判长、检录裁判、加密裁判、现场裁判、评分裁判组成。其中，裁判长由赛项执委会推荐、赛区执委会确认；加密裁判、检录裁判由赛项承办校邀请校外专业教师担任；赛前在赛项裁判员库中随机抽取既定数量的现场裁判和评分裁判。

赛项所需现场裁判和评分裁判的具体要求如下：

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

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

该赛项为2011年-2018年连续举办八年的国赛项目，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。

**附件一：**

**2019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**

**样卷**

赛项时间

9:00-15:00，共计6小时，含赛题发放、收卷及午餐时间。

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  平台搭建与安全设备配置防护 | 任务1 | 网络平台搭建 | 9:00-13:30 | 60 |
| 任务2 | 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1 | XSS渗透测试与安全开发 | 60 |
| 任务2 | 密码学与IPSec应用 | 60 |
| 任务3 | Web应用渗透测试与安全开发 | 60 |
| 任务4 | ICMP扫描渗透测试 | 60 |
| 任务5 | 逆向分析和缓冲区溢出渗透测试 | 80 |
| 任务6 | 云服务安全渗透测试 | 80 |
| 中场收卷 | | | 30分钟 | |
| 第三阶段  分组对抗 | 系统加固 | | 15分钟 | 300 |
| 系统攻防 | | 45分钟 |

赛项内容

本次大赛，各位选手需要完成三个阶段的任务，其中第一个阶段需要按裁判组专门提供的U盘中的“XXX-答题模板”提交答案。第二、三阶段请根据现场具体题目要求操作。

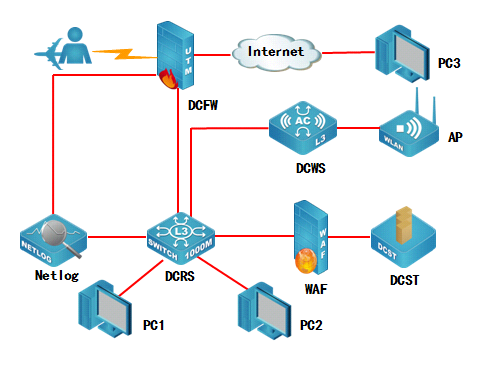
选手首先需要在U盘的根目录下建立一个名为“GWxx”的文件夹（xx用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

特别说明：只允许在根目录下的“GWxx”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

网络拓扑图



IP地址规划表

|  |  |  |  |
| --- | --- | --- | --- |
| **设备名称** | **接口** | **IP地址** | **对端设备** |
| 防火墙DCFW | ETH0/2 | 10.0.0.1/30 | DCRS |
| ETH0/1 | 218.5.18.1/27 | PC（218.5.18.2） |
| L2TP | 192.168.10.1/24  可用IP数量为20 | L2TP地址池 |
| ETH0/3 | 10.0.0.10/30 | Netlog |
| 无线控制器DCWS | VLAN 1002  ETH1/0/1 | 10.0.0.6/30 | DCRS |
| ETH1/0/2 |  | AP |
| 管理VLAN  VLAN 100 | 192.168.100.254/24 |  |
| VLAN 101  ETH1/0/11-24 | 192.168.101.1/24 |  |
| WEB应用防火墙WAF | ETH2 | 172.16.100.2/24 | DCST |
| ETH3 | DCRS |
| 三层交换机DCRS | VLAN 1001  ETH1/0/2 | 10.0.0.2/30 | DCFW |
| VLAN 1002  ETH1/0/1 | 10.0.0.5/30 | DCWS |
| VLAN 10 | 172.16.10.1/24 | 无线2 |
| VLAN 20 | 172.16.20.1/25 | 无线1 |
| 无线管理VLAN  VLAN 30 | 172.16.30.1/26 |  |
| VLAN 40  ETH1/0/6-9 | 192.168.40.1/24 | PC1 |
| 管理VLAN  VLAN 100 | 192.168.100.1/24 |  |
| VLAN 200  ETH1/0/10-24 | 172.16.100.1/24 | WAF、PC2 |
| 日志服务器DCBI-Netlog | ETH2 | 10.0.0.9/30 | DCFW |
| ETH3 |  | DCRS(ETH1/0/4) |
| 堡垒服务器DCST | - | - | WAF |

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-Netlog | https://192.168.5.254 | ETH0 | admin | 123456 |
| WEB应用防火墙WAF | https://192.168.45.1 | ETH5 | admin | admin123 |
| 三层交换机DCRS | - | Console | - | - |
| 无线交换机DCWS | - | Console | - | - |
| 堡垒服务器DCST | - | - | 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）**

### 任务1：平台搭建要求如下（60分）：

|  |  |
| --- | --- |
| **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-Netlog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，在DCRS交换机上创建相应的VLAN，并将相应接口划入VLAN。 |
| 7 | 采用静态路由的方式，全网络互连。 |
| 8 | 防火墙做必要配置实现内网对外网访问 |

### 任务2：网络安全设备配置与防护（240分）

#### DCFW:

1. 在DCFW上配置，连接LAN接口开启PING,HTTP,HTTPS，telnet功能，连接Internet接口开启PING、HTTPS功能；连接Netlog接口为DMZ区域，合理配置策略，让内网用户能通过网络管理Netlog;
2. DCFW配置 LOG，记录NAT会话， Server IP为172.16.100.10.开启DCFW上SNMP服务，Server IP 172.16.100.10 团体字符为public5;
3. DCFW做相应配置，使用L2TP方式让外网移动办公用户能够实现对内网的访问，用户名密码为dcn2015， VPN地址池参见地址表；合理配置安全策略。
4. 出于安全考虑，无线用户移动性较强，无线用户访问 Internet是需要采用实名认证，在防火墙上开启Web认证，账号密码为2015web;
5. 为了合理利用网络出口带宽，需要对内网用户访问Internet进行流量控制，园区总出口带宽为200M，对除无线用户以外的用户限制带宽，每天上午9:00到下午6:00每个IP最大下载速率为2Mbps，上传速率为1Mbps；
6. DCFW上配置NAT功能，使PC3能够通过Web方式正常管理到AC，端口号使用6665;）合理配置安全策略;
7. 在DCFW做相关配置要求防火墙能够记录每天9:00-18:00内网用户访问外网的URL，保存在日志服务器；
8. 配置防火墙Web外发信息控制策略，禁止内网无线用户到所有网站的Web外发信息控制；内网有线用户到外网网站Web外发信息控制，禁止外发关键字“攻击”“病毒”，信任值为1，并记录相关日志。
9. DCFW做相关配置要求内网用户不能登录QQ和MSN；
10. DCFW上配置限制内网用户访问www.sohu.com 限制内网用户访问URL中带有sohu关键字的所有网站;

#### Netlog:

1. 在DCBI-netlog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;要求对内网访问Internet全部应用进行记录日志;
2. 在DCBI-netlog上配置，监控周一至周五9：00-18：00 无线用户所在网段访问的URL中包含sohu的HTTP访问记录，并且邮件发送告警;
3. 在DCBI-netlog上配置，添加内容规则，对于网站访问关键字包含“搜狐”的，记录并邮件报警；
4. 在DCBI-netlog上配置，使DCBI能够通过邮件方式发送告警信息，邮件服务器IP 172.16.100.20，端口号25，账号test5dcn，密码test5，当DCBI磁盘使用率超过90%时发送一次报警；
5. 在DCBI-netlog上配置，将DCBI的日志信息发送到日志服务器，日志服务器IP 172.16.100.10，community名字public3；
6. 在DCBI-netlog上配置，增加非admin账户DCN2015，密码dcbi5555，该账户仅用于用户查询设备的日志信息和统计信息；
7. DCBI-netlog配置应用及应用组“P2P下载”，UDP协议端口号范围40500-42000，在周一至周五9：00-18：00监控LAN中所有用户的“P2P下载”访问记录并告警；

#### WAF:

1. 在WAF上配置，公司内部有一台网站服务器直连到WAF，IP地址是172.16.100.30，端口是8080，并将服务访问日志、Web防护日志、服务监控日志发送至syslog日志服务器，syslog日志服务器IP地址是172.16.100.10，UDP的514端口;
2. 在公司总部的WAF上配置，将攻击告警、设备状态告警信息通过邮件（发送到DCN@digitalchina.com）及短信方式(发送到13913814949)发送给管理员;
3. 在公司总部的WAF上配置，禁止公网IP地址（218.5.18.2）访问网站服务器，网站服务器IP地址是172.16.100.30；
4. 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：并发访问超过3000次请求；
5. 在WAF上配置，开启基于 session cookie的CC防护，最大请求数为3000，超过进行阻止;

#### 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25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；连接PC1的接口为专用接口，限定只允许PC1的MAC地址可以连接；
2. 将连接DCFW的双向流量镜像至Netlog进行监控和分析；
3. 开启防ARP扫描功能，单位时间内端口收到ARP数量超过50便认定是攻击，DOWN掉此端口；
4. 在公司总部的DCRS上配置端口环路检测（Loopback Detection），防止来自VLAN200接口下的单端口环路，并配置存在环路时的检测时间间隔为30秒，不存在环路时的检测时间间隔为10秒;
5. 为了控制接入网络PC，需要在交换ETH1/0/10口开启DOT1X认证，配置认证服务器，IP地址是172.16.100.40，radius key是dcn2015;
6. 交换机开启远程管理，使用SSH方式账号为DCN2015，密码为555555;
7. VLAN20、VLAN30、VLAN10 用户采用动态获取IP地址方式，DHCP服务器在AC上配置，前十个地址为保留地址，VLAN40用户也动态获取IP，DHCP server为DCFW;
8. 在交换机上配置，在只允VLAN200用户在上班时间（周-到周五8:00到18:00）内访问VLAN100段IP;
9. 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，VLAN30用户的ARP阀值为50;
10. 为了防止VLAN40网段arp欺骗，需要在交换机上开启ip dhcp snooping并在接口下绑定用户;
11. 在DCRS上配置，配置设备enable密码，密码为dcn2015，并且在登录设备时必须正确输入enable密码才能进入交换机的配置模式;
12. DCRS上配置，VLAN40的成员接口开启广播风暴抑制功能，参数设置为2500pps;

#### DCWS：

1. AP通过option43方式进行正常注册上线,hwtype 值为59,AC地址为管理VLANIP；
2. 设置SSID DCN2015，VLAN10，加密模式为wpa-personal,其口令为GSdcn2015的；

设置SSID dcntest ，VLAN20不进行认证加密,做相应配置隐藏该ssid；

1. dcntest最多接入20个用户，用户间相互隔离，并对dcntest网络进行流控，上行速率1Mbps，下行速率2Mbps；
2. 通过配置避免接入终端较多且有大量弱终端时，高速客户端被低速客户端“拖累”，低速客户端不至于长时间得不到传输；
3. 通过配置防止多AP和AC相连时过多的安全认证连接而消耗CPU资源，检测到AP与AC在10分钟内建立连接5次就不再允许继续连接，两小时后恢复正常;
4. AC开启Web管理，账号密码为DCN2015；

**第二阶段任务书（400分）**

### 任务1：XSS渗透测试与安全开发（60分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

物理机操作系统：Windows7 64位旗舰版

虚拟机操作系统1：Ubuntu Linux 32bit

虚拟机操作系统1安装工具1：Python3

虚拟机操作系统1安装工具2：WireShark

虚拟机操作系统1安装工具3：GCC

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

用户名：root，密码：123456

虚拟机操作系统2：CentOS Linux 5.5

虚拟机操作系统安装工具1：GCC

虚拟机操作系统安装工具2：GDB

用户名：root，密码：123456

靶机：

服务器场景：Web Server

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；

**任务内容：**

1. Web访问靶机服务器场景，完成如下任务：a、进入"/"->" Employee Message Board"页面，对该页面进行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"/"->" Employee Message Board"页面存在XSS注入点；b、进入靶机服务器场景的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，填写insert.php程序当中空缺的FLAG01字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
2. 继续修改本任务题目1中的insert.php源程序，使之可以抵御XSS渗透测试，填写insert.php程序当中空缺的FLAG02字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
3. 继续修改本任务题目1中的insert.php源程序，使之可以抵御XSS渗透测试，填写insert.php程序当中空缺的FLAG03字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
4. 继续修改本任务题目1中的insert.php源程序，使之可以抵御XSS渗透测试，填写insert.php程序当中空缺的FLAG04字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
5. 继续修改本任务题目1中的insert.php源程序，使之可以抵御XSS渗透测试，填写insert.php程序当中空缺的FLAG05字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
6. 继续修改本任务题目1中的insert.php源程序，使之可以抵御XSS渗透测试，填写insert.php程序当中空缺的FLAG06字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；

### 任务2：密码学与IPSec应用（60分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

物理机操作系统：Windows7 64位旗舰版

虚拟机操作系统：Microsoft Windows2003 Server

虚拟机操作系统安装工具1：Microsoft Windows CA服务

虚拟机操作系统安装工具2：WireShark1.1

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

用户名：administrator，密码：123456

靶机：

服务器场景：Windows Server

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

**任务内容：**

1. 通过IPSec传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库user表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件WireShark对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景Web页面login.php之后，对攻击机登录靶机Web站点动作的数据对象进行分析，将ISAKMP主模式第1个数据对象长度十进制数值通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
2. 通过IPSec传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库user表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件WireShark对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景Web页面login.php之后，对攻击机登录靶机Web站点动作的数据对象进行分析，将ISAKMP主模式第2个数据对象长度十进制数值通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
3. 通过IPSec传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库user表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件WireShark对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景Web页面login.php之后，对攻击机登录靶机Web站点动作的数据对象进行分析，将ISAKMP快速模式第1个数据对象长度十进制数值通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
4. 通过IPSec传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库user表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件WireShark对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景Web页面login.php之后，对攻击机登录靶机Web站点动作的数据对象进行分析，将ISAKMP快速模式第2个数据对象长度十进制数值通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
5. 通过IPSec传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库user表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件WireShark对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景Web页面login.php之后，对攻击机登录靶机Web站点动作的数据对象进行分析，将ISAKMP快速模式第3个数据对象长度十进制数值通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
6. 通过IPSec传输模式保护保护从攻击机到靶机之间的全部流量（预共享密钥：www.dcn.com），使用靶机数据库user表中第一条记录中的用户名、密码信息登录靶机网站，打开攻击机工具软件WireShark对攻击机和靶机之间的数据对象进行捕获；成功登录靶机服务器场景Web页面login.php之后，对攻击机登录靶机Web站点动作的数据对象进行分析，将ISAKMP快速模式第4个数据对象长度十进制数值通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；

### 任务3：Web应用渗透测试与安全开发（60分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

物理机操作系统：Windows7 64位旗舰版

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具1：Python3

虚拟机操作系统安装工具2：WireShark

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

用户名：root，密码：123456

虚拟机操作系统2：CentOS Linux 5.5

虚拟机操作系统安装工具1：GCC

虚拟机操作系统安装工具2：GDB

用户名：root，密码：123456

靶机：

服务器场景：Windows Server

服务器场景操作系统：Microsoft 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

**任务内容：**

1. 以HTTP会话方式打开DCN模拟网站主页，继续点击超链接进入DCN产品中心页面，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MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
2. 从靶机服务器场景FTP服务器中下载文件productinfo.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FLAG01字符串，将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
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FLAG02字符串，将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
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FLAG03字符串，将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
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FLAG04字符串，将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
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FLAG05字符串，将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
7. 将编辑好后的productinfo.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1题中使用的Web应用程序渗透测试方法对靶机进行渗透测试，将此时Web页面弹出的字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；

### 任务4：ICMP扫描渗透测试（60分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

物理机操作系统：Windows7 64位旗舰版

虚拟机操作系统：Ubuntu Linux 32bit

虚拟机操作系统安装工具1：Python3

虚拟机操作系统安装工具2：WireShark

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

用户名：root，密码：123456

虚拟机操作系统2：CentOS Linux 5.5

虚拟机操作系统安装工具1：GCC

虚拟机操作系统安装工具2：GDB

用户名：root，密码：123456

靶机：

服务器场景：Windows Server

服务器场景操作系统：Microsoft 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

**任务内容：**

1. 从靶机服务器场景的FTP服务器中下载文件scan02.py，编辑该Python3程序文件，使该程序实现从攻击机对靶机进行的ICMP类型的主机在线探测渗透测试，填写该文件当中空缺的FLAG01字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
2. 继续编辑该任务题目7中的Python3程序文件scan02.py，使该程序实现从攻击机对靶机进行的ICMP类型的主机在线探测渗透测试，填写该文件当中空缺的FLAG02字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
3. 继续编辑该任务题目7中的Python3程序文件scan02.py，使该程序实现从攻击机对靶机进行的ICMP类型的主机在线探测渗透测试，填写该文件当中空缺的FLAG03字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
4. 继续编辑该任务题目7中的Python3程序文件scan02.py，使该程序实现从攻击机对靶机进行的ICMP类型的主机在线探测渗透测试，填写该文件当中空缺的FLAG04字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
5. 继续编辑该任务题目7中的Python3程序文件scan02.py，使该程序实现从攻击机对靶机进行的ICMP类型的主机在线探测渗透测试，填写该文件当中空缺的FLAG05字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
6. 通过Python3程序解释器执行程序文件scan02.py，将该程序文件执行后的显示结果中，找到对应的字符填入以下形式（最后1行的第1个字符:最后1行的最后1个字符），并将该形式字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；

### 任务5：逆向分析和缓冲区溢出渗透测试（80分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

物理机操作系统：Windows7 64位旗舰版

虚拟机操作系统1：Ubuntu Linux 32bit

虚拟机操作系统1安装工具1：Python3

虚拟机操作系统1安装工具2：WireShark

虚拟机操作系统1安装工具3：GCC

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

用户名：root，密码：123456

虚拟机操作系统2：CentOS Linux 5.5

虚拟机操作系统安装工具1：GCC

虚拟机操作系统安装工具2：GDB

用户名：root，密码：123456

靶机：

服务器场景1：Windows Server

服务器场景1操作系统：Microsoft Windows2003 Server

服务器场景1的FTP下载服务用户名：anonymous，密码：123456

服务器场景1的FTP下载服务端口：2121

服务器场景1的FTP上传服务用户名：anonymous，密码：123456

服务器场景1的FTP上传服务端口：21

服务器场景2：LinuxServer

服务器场景2操作系统：CentOS Linux 5.5

**任务内容：**

1. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG01中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
2. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG02中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
3. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG03中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
4. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG04中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
5. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG05中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
6. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG06中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
7. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG07中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
8. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG08中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
9. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG09中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
10. 从靶机服务器场景的FTP服务器中下载可执行文件OverFlow，通过攻击机调试工具，对以上可执行文件进行逆向分析；通过缓冲区溢出渗透测试方法对服务器场景2的TCP：4444端口进行渗透测试，获得靶机根路径下的文件FLAG10中的字符串，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；

### 任务6：云服务安全渗透测试（80分）

**任务环境说明：**

攻击机：

注意：攻击机须使用物理机中的虚拟机

物理机操作系统：Windows7 64位旗舰版

虚拟机操作系统1：Ubuntu Linux 32bit

虚拟机操作系统1安装工具1：Python3

虚拟机操作系统1安装工具2：WireShark

虚拟机操作系统1安装工具3：GCC

虚拟机网卡与物理机网卡之间的关系：Bridge（桥接）

用户名：root，密码：123456

虚拟机操作系统2：CentOS Linux 5.5

虚拟机操作系统安装工具1：GCC

虚拟机操作系统安装工具2：GDB

用户名：root，密码：123456

靶机：

服务器场景1：Windows Server

服务器场景1操作系统：Microsoft Windows2003 Server

服务器场景1的FTP下载服务用户名：anonymous，密码：123456

服务器场景1的FTP下载服务端口：2121

服务器场景1的FTP上传服务用户名：anonymous，密码：123456

服务器场景1的FTP上传服务端口：21

服务器场景2：Windows 7

服务器场景2操作系统：Microsoft Windows 7

**任务内容：**

1. 从靶机服务器场景1的FTP服务器中下载文件cloudattack.py，编辑该Python3程序文件，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限；完善cloudattack.py程序文件，填写该文件当中空缺的FLAG01字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
2. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG02字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
3. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG03字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
4. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG04字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
5. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG05字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
6. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG06字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
7. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG07字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
8. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG08字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
9. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG09字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
10. 继续编辑该任务题目1中的Python3程序文件cloudattack.py，使该程序实现通过靶机服务器场景2中某具有0day漏洞的云服务来获得该云服务器的最高权限，填写该文件当中空缺的FLAG10字符串，将该字符串通过MD5运算后返回的哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；
11. 通过Python3程序解释器执行程序文件cloudattack.py，获得靶机服务器场景2中云服务器的最高权限，并打印云服务器根路径下的文件FLAG当中的字符串的内容，并将该字符串通过MD5运算后返回哈希值的十六进制结果作为Flag值提交（形式：十六进制字符串）；

**第三阶段任务书（300分）**

假定各位选手是DCN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。

注意事项：

注意1：任何时候不能人为关闭服务器的服务端口1-1024；

注意2：不能对裁判服务器进行攻击；

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；

注意4：不得人为恶意破坏自己服务器的Flag值；

注意5：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。靶机的Flag值存放在./root/flagxxxxx.txt文件内容当中。每提交1次对手靶机的Flag值增加3分，每当被对手提交1次自身靶机的Flag值扣除3分，每个对手靶机的Flag值只能被自己提交一次。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，各位选手可以继续加固自身的服务器，也可以攻击其他选手的服务器。

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。