山东省“技能兴鲁”职业技能大赛——

第四届山东省移动互联网及5G应用创新技能大赛
网络与信息安全管理员赛项

**技术文件**

为确保山东省“技能兴鲁”职业技能大赛——第四届山东省移动互联网及5G应用创新技能大赛——网络与信息安全管理员赛项的活动能够顺利实施，特制订如下技术文件。

**一、竞赛项目**

山东省“技能兴鲁”职业技能大赛——第四届山东省移动互联网及5G应用创新技能大赛——网络与信息安全管理员赛项

**二、竞赛任务**

本赛项分为职工（教师）组和学生组两个组别。职工（教师）组为个人赛，学生组为团队赛。学生组由2名学生、2名指导教师组成。

职工（教师）组竞赛用时为3个小时，学生组竞赛用时为6个小时。

学生组竞赛限定1天内进行，竞赛场次为1场，赛项竞赛时间为6小时。

|  |  |  |  |
| --- | --- | --- | --- |
| **模块编号** | **内容模块** | **竞赛时间****（小时）** | **分值权重** |
| A模块 | 基础设施设置与安全加固 | 3 | 20% |
| B模块 | 网络安全事件响应、数字取证调查和应用安全 | 40% |
| 休息时间（午餐） | 1 |  |
| C模块 | CTF 夺旗-攻击 | 3 | 20% |
| D模块 | CTF 夺旗-防御 | 20% |

职工（教师）组竞赛限定1天内进行，竞赛场次为1场，赛项竞赛时间为3小时。

|  |  |  |  |
| --- | --- | --- | --- |
| **模块编号** | **内容模块** | **竞赛时间****（小时）** | **分值权重** |
| A模块 | 基础设施设置与安全加固 | 2 | 20% |
| B模块 | 网络安全事件响应、数字取证调查和应用安全 | 40% |
| 休息时间 | 0.5 |  |
| C模块 | CTF 夺旗-攻击 | 1 | 20% |
| D模块 | CTF 夺旗-防御 | 20% |

竞赛分为A,B,C,D四个模块，总分满分为1000分，裁判组负责竞赛机考评分和结果性评分，由裁判长负责竞赛全过程。竞赛共计6小时。其中模块A成绩占总成绩的20%，模块B成绩占总成绩的40%，模块C成绩占总成绩的20%，模块D成绩占总成绩的20%。

(一)模块A 基础设施设置与安全加固

此模块通过综合运用登录和密码策略、数据库安全策略、流量完整性保护策略、事件监控策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力。本模块要求对具体任务的操作截图并加以相应的文字说明,并以word文档的形式书写,以PDF格式保存,并以赛位号作为文件名.

(二)模块B 网络安全事件、数字取证调查和应用安全

此模块重点考查选手帮助企业进行调查并追踪本次网络攻击的源头，分析黑客的攻击方式，发现系统漏洞，提交网络安全事件响应报告，修复系统漏洞，删除黑客在系统中创建的后门，并帮助系统恢复正常运行。

(三)模块C CTF夺旗-攻击

此模块重点考查选手针对企业网络中可能存在的各种问题和漏洞。尝试利用各种攻击手段，攻击特定靶机，以便了解最新的攻击手段和技术，了解网络黑客的心态，从而改善防御策略。

(四)模块D CTF夺旗-防御

此模块重点考查处理可能存在着各种问题和漏洞。如何去尽快对这些服务器进行渗透测试与安全防护。每个参赛队拥有专属的堡垒机服务器，其他队不能访问。参赛选手通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能。

 **三、技术平台**

（一）比赛器材

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **设备要求** |
| 1 | 网络安全竞赛平台 | 1 | 1. 能完成基础设施设置、安全加固、安全事件响应、网络安全数据取证、应用安全、CTF夺旗攻击、 CTF夺旗防御等知识、技能内容竞赛环境实现，能有效支持300人规模，具备基于本规程竞赛内容同一场景集中答题环境。2. 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，支持集群管理，同步采用增量备份的方式，虚拟化管理采用标准libvirt接口；支持多用户并发在线竞赛，根据不同的实战任务下发进行自动调度靶机虚拟化模板，全程无需手工配置地址，VLAN与IP可根据竞赛要求自行设定；提供单兵闯关、分组混战等实际对战模式，阶段间无需人工切换，系统自动处理；提供超过20种不同级别70个的攻防场景；模块B、C全过程自动评判，支持竞赛过程图像元素上传，排名判定策略大于等于12种；自定义动画态势展示，成绩详细分析；支持监控异常虚拟机，同时检测FTP、HTTP、ICMP、SMTP、SSH、TCP和UDP协议，服务端口支持在有效范围内的服务端口；支持全程加密，支持加密文件导入，加密方式为非对称加密，设备能随机生成密码。 |
| 2 | PC机 | 2 | CPU 主频>=2.8GHZ,>=四核四线程；内存>=8G；硬盘>=500G；支持硬件虚拟化。 |

（二）软件技术平台：

竞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：微软 Windows 7(64位)中文试用版或微软 Windows 10(64位)中文试用版。

2．虚拟机安装操作系统：

Windows系统（试用版）：Windows XP、Windows 7、Windows 10、Windows Server2003及以上版本（根据命题实际确定）。

Linux系统：Ubuntu、Debian、CentOS（具体版本根据命题实际确定）。

3.其他主要应用软件为（实际竞赛环境可能不仅限于以下软件）:

VMware workstation 12 pro 及以上版本免费版

Putty 0.67及以上版本

Python 3及以上版本

Chrome 浏览器 62.0及以上版本

RealVNC 客户端 4.6及以上版本

**四、成绩评定**

（一）裁判工作原则

裁判长由赛项执委会推荐，赛前建立健全裁判组。裁判组为裁判长负责制，并设有专职督导人员1-2名，负责比赛过程全程监督，防止营私舞弊。

本赛项拟设裁判5-6名。分为裁判长、加密裁判（2名）、现场裁判。

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

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

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

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

 （二）裁判评分方法

裁判组负责竞赛机考评分和结果性评分，由裁判长负责竞赛全过程。

竞赛现场派驻监督员、裁判员、技术支持队伍等，分工明确。裁判员负责与参赛选手的交流沟通及试卷等材料的收发，负责设备问题确认和现场执裁；技术支持工程师负责所有工位设备应急，负责执行裁判确认后的设备应急处理。

（三）成绩产生办法

1.评分阶段：

|  |  |  |  |
| --- | --- | --- | --- |
| **竞赛阶段** | **阶段名称** | **任务阶段** | **评分方式** |
| 模块A权重20% | 基础设施设置、安全加固 | 任务1…N | 裁判客观评分 |
| 模块B权重40% | 安全事件响应、网络安全数据取证、应用安全 | 任务1…N  | 机考评分 |
| 模块C权重20% | CTF夺旗攻击、  | 系统攻防演练 | 机考评分 |
| 模块D权重20% | CTF夺旗防御 | 系统攻防演练 | 裁判客观评分 |

2.模块A、模块B评分规则

模块A与模块B总分为600分,分为N个任务，每道题的具体分值在赛题中标明；模块A基础设施设置、安全加固部分评分由评分裁判客观评分；模块B安全事件响应、网络安全数据取证、应用安全等部分由系统自动评分和排名。

3.模块C、模块D评分规则

模块C总分为200分，按照选手获得攻击“FLAG”的值得到相应的分数。系统自动评分和排名。

模块D总分为200分，按照选手答题内容，由评分裁判进行客观评分。

4.选手在答题过程中不得违反竞赛试题要求答题，不得以违规形式获取得分，不得违规攻击裁判服务器、网关、系统服务器等非靶机目标，如检测选手有违规攻击行为，警告一次后若继续攻击，判令该队终止竞赛，清离出场。