关于举办2020年全省

网络安全管理员职业技能大赛的通知

附件1

全省网络安全管理员职业技能大赛组委会名单

一、组委会领导

主 任：

张仲茜 陕西省总工会党组副书记、常务副主席

高彩玲 陕西省通信管理局党组书记、局长

副主任：

刘 伟 陕西省总工会党组成员、经审会主任

李林栋陕西省通信管理局党组成员、副局长
 吕海涛 陕西省公安厅副厅级侦察员
 张利原 中国人民银行西安分行党委委员、工会主任

向 涛 中国铁塔陕西省分公司党委书记、总经理，陕西省信息通信行业协会理事长

成 员：

苏秀梅 陕西省职工创新技术协作中心副主任

朱 军 陕西省通信管理局网络安全管理处处长

杜建龙 陕西省通信行业职业技能鉴定中心主任

国创锋 陕西省通信管理局办公室副主任 （主持工作）

刘 凯 陕西省公安厅网络安全保卫总队总队长

董晓北 陕西省信息通信行业协会秘书长

高 卫 中国电信股份有限公司陕西分公司网络与信息安全部总经理

苏宇楼 中国移动通信集团陕西有限公司信息安全部总经理

袁知明 中国联合网络通信有限公司陕西省分公司信息安全部总经理

董召军 中国铁塔股份有限公司陕西省分公司业务支撑部总经理

二、工作机构

（一）技术保障组：负责竞赛命题。竞赛平台环境设计及搭建，保障竞赛顺利进行。

组 长：赵湘楠

成 员：刘 凯 代长生 张丽荣

（二）裁判组：保障竞赛的公平公正。

组 长：朱 军

成 员：徐洪魁 阿合买提·雨三 代亚飞 王伯英

（三）仲裁组：负责竞赛争议的仲裁。

组 长：苏秀梅

成 员：代亚飞 吕西平 王伯兴 孙鹏飞 王海山

李 晖

（四）综合组：负责竞赛活动宣传报道。

组 长：董晓北

成 员：张丽荣 薛 冲 杨明泽

（五）会务服务组：负责竞赛报名、综合协调及场地。

组 长：谢 红

成 员：张丽荣 代长生

附件2

全省网络安全管理员职业技能大赛初赛规则

一、比赛形式

1.大赛采用“信息安全理论知识+CTF解题赛”模式，比赛分理论知识和实际操作两部分，分别占总成绩的30%和70%。

2.理论赛时间为1个小时，CTF解题赛时间为5小时。

二、报名规则

1.报名时间：2020年8月10日-8月14日。

2.报名方式：登录陕西省信息通信行业协会官网（http://www.scia.org.cn），点击2020陕西省网络安全管理员职业技能大赛/报名系统，注册报名和登录。

3.每支参赛队伍由三人组成，一名队长两名队员，由参赛者单位组织统一进行报名注册。

4.注册所有信息务必填写正确，提交报名信息并通过审核，则视为报名成功。

5.报名所填信息必须真实，提交虚假信息者一经查实取消单位参赛资格。

6.参赛队伍名称可自行设计，不得违反国家相关法律法规要求和社会公德，不得侵犯他人品牌权利、知识产权、名誉权等合法权利，不得使用侮辱性、低俗、色情等词汇。对违反此规定的大赛组委会有权要求参赛队伍修改名称、队伍标识。

7.在报名截止前若需修改队伍信息，由参赛单位联系大赛组委会办公室进行变更。

8.报名信息确认工作截止到2020年8月16日，之后不可变更队员信息，不得更换或增加队员。

9.报名成功后参赛选手可登录[陕西省信息通信行业协会官网2020年陕西省网络安全管理员职业技能大赛/学习系统进行学习，平台开放时间2020年8月17日至2020年8月3](http://xxxxxx）进行学习，平台开放时间2020年7月30日至2020年8月12)0日，学习期间有任何疑问可联系大赛组委会办公室。

三、比赛规则

1.比赛过程中参赛团队严禁向比赛答题平台等发起任何可能影响比赛的攻击行为,一经发现取消参赛资格。

2.比赛过程中严禁任何作弊行为，一经发现取消参赛资格。

3.比赛过程中以裁判长牵头的仲裁意见为最终裁决。

4.比赛结束后6小时内，各参赛队伍提交writeup，过期视为放弃比赛成绩。

四、惩罚规则

有违反上述规定者，大赛组委会视情节轻重给予警告、扣分、公开警告、终止比赛资格，并通报所在单位。

注：比赛规则的解释权归大赛组委会所有。规则中未作明确说明的事项，大赛组委会保留最终解释权。

附件3

决赛线下培训课程表

|  |  |  |
| --- | --- | --- |
| **时间** | **大纲** | **内容** |
| 9月10日 | 学员报到 | 所有学员到陕西通信技师学院（西安市长安区郭杜镇杜回村甲字2号）报到。 |
| 9月11日上午 9:00-12:00 | 网络攻防上 | 1、介绍Linux的必备命令和Linux权限管理知识。 |
| 2、线下AWD攻防赛中常用套路和组合命令使用技巧。 |
| 3、AWD攻防赛中不死马脚本编写技巧。 |
| 4、攻防赛Python脚本编写技巧。 |
| 5、CMS在线下AWD攻防赛中的攻击与防御。 |
| 6、攻防赛中PWN攻击与防御。 |
| 7、竞赛中常见组件和常见服务漏洞的利用方法与攻防思路。 |
| 9月11日下午 14：00-17:00 | 网络攻防下 | 1. 常见web框架漏洞介绍及利用 |
|  - ThinkPHP（PHP） |
|  - Laravel（PHP） |
|  - Django（python） |
|  - Flask（python） |
|  - struts（java） |
| 2. AWD攻防攻击框架介绍 |
|  - 批量化payload攻击 |
|  - 批量化提交flag |
|  - 攻击脚本的编码、混淆 |
|  - webshell、不死马植入 |
| 3. AWD防御： |
|  - 快速备份与漏洞检测 |
|  - 各类web漏洞修复、加固方法 |
|  - 文件监控 |
|  - 分析payload流量 |
| 9月11日晚上 19:00-21:00 | 晚自习+互动答疑 |
|
| 9月12日上午 9:00-12:00 | 安全运维-加固/监测 | 1. 文件安全、账户安全、权限控制 |
| 2. linux安全策略、防火墙 |
| 3. 系统漏洞检测与修复 |
| 4. 系统服务加固 |
| 5. 系统日志分析 |
| 6. Web中间件日志分析 |
| 7. 异常流量分析 |
| 9月12日下午 14:00-17:00 | 安全运维-治理/应急 | 1. webshell检测与治理 |
| 2. 系统后门检测与治理 |
| 3. 了解rootkit及rootkit治理 |
| 4. 了解反弹shell和端口转发 |
| 5. 后门的持久化存留 |
| 6. 常见应急响应事件分析 |
| 7. 应急响应场景实践（挖矿后门、恶意植马、脱库） |
| 9月12日晚上 19:00-21:00 | 晚自习+互动答疑 |
|
| 9月13日上午 9:00-12:00 | 新技术新方向 | 1. 5G安全 |
| 2. 云计算安全 |
| 3. 工控安全 |
| 4. 大数据安全 |
| 5. 区块链安全 |
| 9月13日下午14：00-17:00 | 解题相关讲解 | 1. 文件修复、压缩包分析 |
| 2. 图片、音频、文档隐写分析 |
| 3. 各类编码分析（莫尔斯电码、base64系列、url编码、二维码、进制转换等） |
| 4. 对称密码 |
| 5. 公钥密码 |
| 6. 数字签名相关知识、赛题 |
| 7. 逆向工程中的静态分析与动态调试 |
| 8. 分析PE文件、ELF文件 |
| 9. 去除花指令、程序的查壳与脱壳 |
| 10. 反调试技术绕过、加密算法的逆向 |

此次培训收取培训费3600元/人（含培训期间食宿费用），会务组统一安排食宿。

送：陕西省公安厅、中国人民银行西安分行

|  |
| --- |
| 陕西省总工会办公室 2020年7月27日印发  |