附件1

六安市第二届网络安全技能大赛

技术说明文档

为保证六安市第二届网络安全技能大赛顺利进行，现将本次大赛有关技术文件内容说明如下，请参照执行。

一、大赛职业

网络和信息安全管理员

二、大赛标准

根据《中华人民共和国职业分类大典（2022年版）》中网络和信息安全管理员的职业定义和描述，以充分发挥信息安全人才的积极性和创造力，重点考察计算机安全与网络攻防的知识与技能，提升信息安全意识，普及信息安全知识，实践信息安全技术为目的，做好网络安全与信息化人才的选拔储备工作。

三、大赛内容

大赛分为线上选拔赛、线下决赛两个阶段，线上选拔赛比赛内容为理论知识，线下决赛比赛内容理论知识占40%、技能操作占60%，均通过Web访问竞技系统方式进行。参赛选手报名成功后，获得比赛账号，在指定时间内完成作答。

**（一）理论知识竞赛**

理论知识题目类型为选择题，主要根据日常运维及工作需要，考察选手日常的安全意识、安全运维、等级保护及安全攻防等技能，分为单选题、多选题，涉及安全管理、安全体系模型、安全设计运维、物理安全、网络安全、系统安全、应用安全、数据安全、密码学、恶意代码、移动终端安全、安全工具等多个方向。

题型分别为单项选择题、多项选择题。其中：单项选择题40道，每题3分，共120分；多项选择题20道，每题4分，共80分，总分200分。合计60道试题，比赛时长1小时。

**（二）技能操作竞赛**

技能操作竞赛类型为CTF（Capture The Flag，信息安全夺旗赛）比赛，题目类型包括： WEB（渗透测试）、CRYPTO（密码学）、PWN（漏洞利用）、REVERSE（逆向工程）、MISC（安全杂项）等，共10道题，总分200分，比赛时长为2小时。

**1、题目范围**

题目数量：共10道题目，视答题情况开启附加题。

难度设置：难度等级为高、中、低。难度分布为高（30%）、中（40%）、低（30%）。

|  |
| --- |
| **CTF竞赛模式名词介绍** |
| **类型名称** | **类型内容介绍** |
| WEB | 题目会涉及常规的漏洞及部分渗透测试相关性题目。 |
| MISC | 安全杂项，可能涉及流量分析、各种网络取证、社会工程学、数据分析等类型。 |
| CRYPTO | 密码学，考察各种加解密技术，算法等。 |
| PWN | 常为溢出类题目。 |
| REVERSE | 逆向工程，主要涉及软件逆向、破解等技术。 |

**2、知识大纲**

包括Web安全、密码学、逆向工程、安全杂项、溢出等，知识技能大纲至少包含如下内容：

分值设置：CTF赛题根据题型难易程度，每题分值为10—30分不等，总分200分。

竞赛规则：CTF模式题型有且不限于：WEB、CRYPTO、PWN、REVERSE、MISC五大类别。

|  |  |
| --- | --- |
| **类型** | **CTF知识体系大纲** |
| Web安全信息泄露 | 代码审计Cookie伪造、社会工程、命令注入、 XSS盲打、端口扫描 、x-forwarded-for绕过限制、orderby注入、SQL注入、搜索型SQL注入、SSRF漏洞、CSRF漏洞、 PHP反序列化、WAF绕过漏洞、暴力破解、目录遍历、文件包含、任意代码执行、文件上传漏洞、任意文件下载、弱口令、隐藏字段、robots.txt、j2ee框架漏洞、Struts2框架漏洞、PHP反序列化、ZIP://伪协议漏洞、TOMCAT漏洞、权限漏洞、业务逻辑支付漏洞、旁注漏洞、JS前端校验等。 |
| Crypto密码学 | DES、奇偶校验（汉明码）、算法、算法编程、文件格式、jother、移位密码、频率分析、维吉尼亚解密、Windows密码、Rabin加密算法、乐谱隐藏、替换密码、频率攻击、base64解密、md5破解、栅栏密码、猪圈密码、RAR破解、四方密码、中文电码、RSA共模攻击、维吉尼亚、频率攻击等。 |
| Misc安全杂项 | 图片隐写、LSB水印算法隐藏、二维码技术、音频分析、摩斯电码、ZIP暴力破解、数据分析、网络分析、二进制取证分析、网络抓包分析、Base64解密、APK逆向分析、APK木马分析、Webshell 查杀、编程、社会工程、编程、应急响应、文件头修改、文件头修复、图片分离、pngcheck、摩斯电码等。 |
| Reverse逆向工程 | EXE程序逆向、APK逆向、算法分析、固件逆向、注册机逆向、逆向算法、JAVA逆向、JAVA编程、脱壳、IDA分析、脱壳技术等。 |
| Pwn溢出 | Linux本地、Windows本地、远程溢出，二进制文件分析、溢出代码编写、IDA分析、NC反弹技术等。 |

四、比赛要求

1、题目可能涉及靶机或相关的文件，选手通过直接访问靶机或者下载相关题目文件进行解题；

2、解题后将答案提交至评分系统，评分系统将自动判断答案，若回答正确将获得相应分值；

3、按解题时间排序，第一名、第二名、第三名成功解答题目的选手将获得一定的加分（按照题目分值的30%、20%、10%）；

4、大部分flag为此形式：FLAG｛可见字符串｝；如果flag为其他形式，题目中会单独说明；

5、积分相同时，根据最后一道得分题目提交时间，先提交者名次高；

6、若某道题目长时间没有选手能解出时，组委会将适时发布提示信息；

7、选手若发现大赛平台或者赛题有非预期漏洞并通报组委会时，组委会会酌情加分；

8、禁止任何对比赛相关平台的暴力破解和攻击，违规者一律取消参赛资格；

9、当比赛结束后，所有参赛选手获得flag将无法在平台内提交，组委会将不再接受所有参赛选手以任何形式提交flag；

10、参赛选手注册信息中，请不要含有违背国家相关政策法规内容，并避免有低俗、暴力、色情、脏话等词汇，如发现将立即删除账号并取消参赛资格。

五、大赛成绩

大赛总成绩由理论知识和实际操作两部分成绩共同组成。理论知识和实际操作均为总分400分。理论知识成绩占总成绩的40%。实际操作成绩占总成绩的60%。依据总成绩高低排出个人名次，当总成绩相同时，以实际操作成绩高者为先。

六、裁判机构与原则

比赛裁判工作遵循公平、公正、公开的原则。本赛项的裁判组成员由本届大赛裁判委员会组建。

七、说明

六安市网络安全技能大赛技术说明文件一切解释权归大赛活动组委会所有。

八、样题

**（一）理论知识**

**1、单选题－法律法规**

（）以下哪一项不是我国与信息安全有关的国家法律。A.《信息安全等级保护管理方法》

B.《中华人民共和国保守国家秘密法》

C.《中华人民共和国刑法》

D.《中华人民共和国国家安全法》

答案：C

**2、单选题－软件安全**

（）是一种自动检测远程或本地主机安全性弱点的程序。

A.杀毒软件

B.扫描器程序

C.防火墙

D.操作系统

答案：B

**3、单选题 -安全管理**

ISMS的审核的层次不包括（）。

A.符合性审核

B.有效性审核

C.正确性审核

D.文件审核

答案：C

**4、多选题－信息科学技术基础**

Linux关机命令包括（）。

A.halt

B.shutdow -h now

C.poweroff

D.init 0

答案：ABCD

**（二）技能操作**

**MISC安全杂项**

（1）题目名称：基础破解

（2）题目描述：FLAG包含在四位数字加密的压缩包中。

（3）解题过程：

下载解压文件



根据提示，解压包的密码是四位的整数，可以利用工具ARCHPR进行破解。

 

爆破成功，拿到密码2563。



解压后打开txt文件。



末尾有=，猜测是base64编码，提交验证得到结果。



Flag为：

flag{70354300a5100ba78068805661b93a5c}