**“安恒杯”南京邮电大学首届CTF网络攻防比赛实施方案**

**2015年10月**

目 录

[1 赛事章程 3](#_Toc434265287)

[1.1 大赛组织机构 3](#_Toc434265288)

[2 技术实施 3](#_Toc434265289)

[2.1 赛事介绍 3](#_Toc434265290)

[2.1.1 比赛时间 3](#_Toc434265291)

[2.1.2 比赛地点 3](#_Toc434265292)

[2.1.3 比赛形式 3](#_Toc434265293)

[2.1.4 比赛模式 4](#_Toc434265294)

[2.1.5 评分规则 5](#_Toc434265295)

[2.1.6 比赛秩序 6](#_Toc434265296)

[3 其它说明 7](#_Toc434265297)

[3.1 奖励措施 7](#_Toc434265298)

[3.2 比赛工具 7](#_Toc434265299)

# 赛事章程

## 大赛组织机构

* **主办单位：南京邮电大学**
* **支持单位：杭州安恒信息技术有限公司**

****

# 技术实施

## 赛事介绍

### **比赛时间**

2015年11月11日 下午1：00至5：00

### **比赛地点**

教2-316信息安全实验室

### **报名方式**

11月9日15:00前发送“学院、专业、学号、姓名”到邮箱 [13584008622@qq.com](mailto:13584008622@qq.com)

组委会收到报名邮件后，会回信确认，如没有收到报名确认信息，请联系组委会。

联系人：陈伟老师 （手机：13584008622）

### **比赛形式**

此次比赛形式为：线下（局域网）个人赛。

### 比赛模式

**攻防夺旗赛**

主办方提供一系列不同类型的赛题，比如上线一个有漏洞的服务、提供一段网络流量、给出一个加密后的数据或经过隐写后的文件等，参赛选手通过解题获得相应题目中的flag（旗标文件），并提交至评分系统，评分系统审核确认flag正确后，将自动将积分传递给选手，以获得相应的分值。

* 赛题类型分类为：WEB、CRYPTO、REVERSE、MISC四大类别。
* 题目可能涉及靶机或相关的文件，用户通过直接访问靶机或者下载相关题目文件进行解题。
* 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。
* 题目数量：共16道题目
* 难度设置：难度等级为高、中、低。难度分布为高（40％）、中（20％）、低（40％）。

|  |  |
| --- | --- |
| **名词介绍** | |
| **类型名称** | **类型内容介绍** |
| Web | 题目会涉及到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 |
| REVERSE | 逆向工程，主要涉及到软件逆向、破解等技术 |

### 评分规则

本次比赛采用积分赛制：比赛会场的大屏幕上实时展示此次比赛的得分情况和排名。

**攻防夺旗赛评分标准**

* 每题分值为100-500分不等。
* 前三名成功解答题目的选手将获得一定的加分（按照题目分值的百分比：30%/10%/5%），第一名解答题目的选手将获得一次开题权；
* 大部分flag为此形式：FLAG{可见字符串}，只需提交花括号内的可见字符串（大小写敏感）；如果flag为其他形式，题目中会单独说明。
* 比赛中裁判有可能抽查获取得分点的方法，如果发现回答有误，疑似非法渠道获取答案的，取消其该项得分，严重者取消比赛资格。
* 比赛过程中，裁判组根据比赛情况发放题目；
* 比赛组与比赛组之间相互单独，不允许进行访问
* 当参赛选手积分相同时，先达到该分数的选手排名靠前；
* 公平起见，只有当没有任何选手解出某题的时候，裁判组才可能发放相关提示；
* 如果参赛选手发现大赛平台或者赛题非预期漏洞，将会酌情给予一定加分奖励；

### 比赛秩序

* 参赛人员需提前准备自带笔记本电脑、电源。资料(包括书籍、电子资料)及移动存储工具；
* 在比赛开始前签到，并提供有效证件（学生证、身份证）以核实身份信息。
* 比赛正式开始后迟到15分钟者不得进入比赛场地；
* 竞赛工位通过事先分派决定，竞赛期间参赛选手不得离开竞赛工位；
* 比赛过程中或比赛后发现问题（包括反映比赛或其它问题），应当示意裁判组，由裁判组进行解答；
* 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；
* 禁止任何针对参赛对手的网络攻击行为，违规者一律取消参赛资格；
* 禁止通过任何网络连接互联网（包含：共享热点）寻求网络外援远程协助答题。违规者一律取消参赛资格。
* 比赛过程中不能相互交流，禁止参赛队伍之间分享任何解题思路及flag，违规者一律取消参赛资格；
* 使用网络扫描器（例如Nikto或者Nessus）不会对解题有帮助；
* 竞赛结束（或提前完成）后，参赛选手要确认已成功提交的所有竞赛文档，在确认后不得进行任何操作。

# 其它说明

## 奖励措施



## 比赛工具

比赛过程中，可能需要用到各类工具进行答题以及提升答题工作效率，可以实现提醒参赛人员本次夺旗赛、攻防赛可能需要用到工具类型如下：

* 协议抓包分析
* 口令破解
* 编码工具
* 破解工具
* …