2019年浙江省网络安全技能竞赛指南

一、竞赛形式及内容

（一）竞赛形式

在我省信息通信行业相关单位从事网络信息安全管理相关工作满3年，经各单位自下而上层层选拔推荐且符合相应职业规定参赛资格条件的在职员工（不含各类院校教师和学生），经工作单位同意后可报名参加竞赛。

（二）决赛内容

竞赛内容由理论考试和实际操作两部分组成。个人竞赛内容以相关职业（工种）《国家职业标准》高级工（国家职业资格三级）要求为基础，并适当增加部分技师（国家职业资格二级）内容及相关新知识、新技能。

1.报到：8月26日下午15:00-17:00

2.个人竞赛

个人上机竞赛设备调试：8月27日10:10至12:50。

实际操作（CTF）：8月27日下午13:30至16:30。

理论考试：8月28日上午10:00至11:30。

3、团体竞赛

团队竞赛：8月28日下午13:30至16:30。

团体竞赛决赛形式为团队攻防。

二、竞赛规则

（一）个人理论考试

闭卷答题模式，题型为单选题、多选题、判断题。

总分：100分

答题时间：90分钟

题目总数：120题

单选题：80道题 分值：0.5分/题 合计40分

多选题：20道题 分值：1.5分/题 合计30分

判断题：20道题 分值：1.5分/题 合计30分

（二）个人实际操作

答题时间：3小时

个人实际操作采用传统的CTF赛制，为解题模式。CTF夺旗赛模式将提供若干不同类型的题目，参赛队伍通过在预设的比赛环境中解决信息安全的技术问题来获取flag并取得相应积分。比赛成绩按积分高低排序，积分相同时按提交时间排序。

赛题设置：

* 赛题类型分类为：WEB、CRYPTO、PWN、REVERSE、MISC五大类别
* 题目数量：共十道题目
* 难度设置：难度等级为高、中、低。难度分布为高（20％）、中（40％）、低（40％）
* 名次解释：

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。

PWN：常为溢出类题目。

REVERSE：逆向工程，主要涉及到软件逆向、破解等技术。

（三）团队对抗

答题时间：3小时

团队对抗：

团队对抗采用攻防兼备模式。与传统网络安全演练的人机攻防不同，该模式下参赛人员互为攻击方和防守方，实现真正的网络攻防对抗（Attack With Defence，攻防兼备）。参赛队在攻防兼备模式下既要防守自己服务器，也要攻击其它参赛队的服务器。此模式既考察学员的攻击能力，也锻炼学员防御能力。攻防兼备模式为每个参赛队提供2个网络场景，包含2台防守服务器和1台flag服务器。各参赛队网络场景相同且网络场景互通。防守服务器上部署有若干漏洞环境，参赛队员可利用管理员提供的防守服务器登陆信息（用户名、口令、IP地址）登陆防守服务器进行安全加固。在演练过程中，攻方利用守方服务器上的任意漏洞成功获取其服务器权限后，可通过其连接到Flag服务器得到Flag。然后将得到的Flag在答题界面提交得分。同时，守方因为未修复漏洞被攻击成功而扣分。

赛题设置：

* 赛题类型分类为：操作系统安全、数据库安全、中间件安全、Web安全
* 题目数量：2套综合靶机环境
* 靶机系统类型：Linux

**三、考场规则**

（一）参加决赛的选手请务必提前30分钟进入考场；参加个人上机决赛、团体对抗赛的选手请务必于8月27日晚18:00-20:00进入考场进行设备调试，确认考试环境。因选手未提前进行设备调试导致考试受到影响的，由考生本人负责。

（二）考生须凭个人身份证等相关证件进入考场。

（三）考试开始30分钟后不得进入考场。发现替考、徇私舞弊、违反现场竞赛规则等违规者，视情节严重程度进行处罚，直至取消本次参赛资格，通报所在单位，且三年之内不得再次参加同类竞赛。

（四）整个竞赛过程中，禁止使用DDoS工具攻击竞赛系统和考题系统，禁止利用扫描器对答题系统进行Web扫描，如有发现则扣分。

（五）考生应按照决赛现场提供的信息配置个人电脑IP地址，并严格按照决赛现场指定的IP地址访问竞赛系统，如使用其它IP地址则无法访问竞赛系统。由于选手原因造成的网络损坏，须承担后果。

（六）考生入场后，需提前测试网络连通性、验证比赛系统账号和口令。如发现网络、电源故障，应第一时间举手询问。

（七）各参赛选手应自带笔记本电脑，屏幕建议配备防窥膜。决赛前考生需自行准备常用网络安全工具软件。

（八）除上机操作时携带的比赛用电脑外，严禁将各种电子、通信、计算、存储、书籍资料或其它设备带进考场。带入考场的要按监考人员的要求关闭电源，不得放置在桌面上。凡发现竞赛过程中使用上述各种设备，立即取消参赛资格。

（九）上机操作时严禁使用无线上网、蓝牙等功能；严禁访问互联网，严禁自建无线局域网。一经发现，立即取消参赛资格。在竞赛期间，竞赛场地内将开启信号干扰器，屏蔽现场的手机信号和WLAN信号，需要选手准备好有线的鼠标和键盘，准备好网络转接器等外置设备，赛场不负责自带物品的检修和排故。

（十）考场内必须保持安静，不准吸烟，不准交头接耳。必须独立思考、独立完成答题。

（十一）上机操作期间，如遇技术故障，应举手询问。

（十二）竞赛期间，请妥善保管好随身贵重物品及竞赛资料，如有特殊情况，请及时与现场监考或工作人员联系。

（十三）禁止携带网络安全类硬件设备进入考场。

（十四）禁止根据渗透得到的权限进行特权数据的更改，对赛事环境造成影响。