第七届四川省职工职业技能大赛-2021 年四川省网络与信息安全职业技能竞赛

技术文件

目录

一、 赛项概述

为进一步增强网络安全意识，加强我省网络安全人才队伍建设，打造安全可信的网络环境，促进我省产业经济持续健康发展，充分发挥职业技能竞赛对高技能人才培养的引领和促进作用，为广大职工切磋技艺、交流经验、提高技能、展现风采搭建平台，经研究，决定于8月开展2021年四川省网络与信息安全职业技能竞赛。此次竞赛为“第七届四川省职工职业技能大赛”网络与信息安全管理员工种的比赛，通过竞赛选拔出优秀选手，组队代表我省参加“第七届全国职工职业技能大赛”。

鉴于参赛选手日常工作的主要职责是保障信息系统安全稳定运行，大赛将从政策法规标准和网络安全风险评估、安全防护、安全应急响应技术等方面，围绕信息系统的事前检测与防护、事中应急与防御、事后取证与溯源等技术要点展开，全方位考核从业职工的网络安全综合能力。

二、竞赛形式

本赛项为个人赛，赛事分为初赛、复赛、决赛三场，初赛采用线上比赛模式，复赛及决赛采用线下集中模式。

（一）初赛

本赛项采用线上比赛模式进行。竞赛前将组织模拟赛，让参赛选

手提前熟悉平台。线上模拟赛不计分值。

1.模拟赛

线上模拟赛分理论赛和 CTF 夺旗赛两场比赛。

时间：2021 年 8 月 9 日

理论赛：10：30-10：50；CTF 夺旗赛：11：00-11：45

方式：线上模拟（互联网络地址通过报名时预留的手机号码，以短信的方式另行通知）

① 理论赛,时长 20 分钟。

单选题 10 题

多选题 10 题

判断题 10 题

② CTF 夺旗赛,时长 45 分钟，共 2 题。

2.线上选拔赛

线上选拔赛分理论赛和 CTF 夺旗赛两场比赛。

时间：2021 年 8 月 11 日

理论赛：10：30-11：10 ；CTF 夺旗赛：13：00-17：00

方式：线上选拔（互联网络地址通过报名时预留的手机号码，以短信的方式另行通知）

① 理论赛

线上选拔赛当天上午进行理论赛，模式为线上答题，时长 40 分

钟，共 100 分，按 30%计算入线上选拔成绩。考点主要包括政策法规标准等法律法规和网络安全技术知识点。

题目总数 75 题，总分 100 分。

单选题 40 题 分值 1 分/题 合计 40 分；

多选题 25 题 分值 2 分/题 合计 50 分；

判断题 10 题 分值 1 分/题 合计 10 分。

② CTF 夺旗赛

下午进行 CTF 夺旗赛，模式为离线下载题及在线测试题，时长 4 小时，共 10 题（首发 8 题，后补 2 题）共 100 分，按 70%计算入线上选拔成绩。考点主要包括：应急响应处置、物联网安全、工控系统安全、Web 安全、数据包分析、密码技术、数据恢复、移动 APK 分析、逆向分析、PWN 等。

CTF 赛制采取动态计分方式进行计分数。

动态计分算法由平台内部编写特定计算方式通过用户设定的最高分、最低分及衰减次数对题目分数进行动态调整，同一题目答题人数越多，分值越低。

注意：如果出现选手同类分值相同的情况，根据答题时间做优先级排名。

（二）复赛

复赛采用线下集中比赛模式，分理论赛和 CTF 夺旗赛两场比赛。

时间：2021 年 8 月 16 日

入场时间：9：00-10：00

地点：青桐城市酒店（羊犀店）

地址：四川省成都市金牛区蜀西路 16 号

理论赛：10:30-11:30；CTF 夺旗赛：13：00-17：00

① 理论赛

复赛当天上午进行理论赛，模式为集中比赛线上答题，时长 1 小时，共 100 分，按 30%计算入复赛成绩。考点主要包括：政策法规标准等法律法规和网络安全技术知识点。

题目总数 80 题，总分 100 分。

单选题 40 题 分值 1 分/题 合计 40 分；

多选题 20 题 分值 2 分/题 合计 40 分；

判断题 20 题 分值 2 分/题 合计 20 分。

② CTF 夺旗赛

复赛当天下午进行 CTF 夺旗赛，模式为集中比赛，离线下载题及在线测试题，时长 4 小时，共 10 题（首发 8 题，后补 2 题）共 100 分，按 70%计算入复赛成绩。考点主要包括：应急响应处置、物联网安全、工控系统安全、Web 安全、数据包分析、密码技术、数据恢复、移动 APK 分析、逆向分析、PWN 等。

CTF 赛制采取静态计分、动态计分和首先破题奖励三种方式进行计分数。其中首先破题奖励机制附加在静态与动态计分方式中同步进行。默认首先破题奖励比例为：

第一名：题目分值*10%；

第二名：题目分值*5%；

第三名：题目分值*3%。

动态计分算法由平台内部编写特定计算方式通过用户设定的最高分、最低分及衰减次数对题目分数进行动态调整，同一题目答题人数越多，分值越低。具体算法如下图所示：

$$a = \max \text{ points}$$

$$b = \min \text{ points}$$

$$s = \text{solve threshold}$$

$$f(x) = \frac{b-a}{s^2}x^2 + a$$

（三）决赛

决赛采用线下集中比赛模式，以 CTF 方式进行。

时间、地点：另行通知

决赛时长 6 小时，模式为线下集中比赛，以 CTF 方式进行，共 14 题（首发 12 题，后补 2 题）。题目主要分两种类型：一是 web 题：线上虚拟出各种环境，例如 Web 攻防、应急响应、蜜罐、物联网攻防、工控网络等场景，选手需要获得权限后提交相关的 Flag 值。二是漏洞题：线上提供虚拟环境由选手进行相关漏洞挖掘，选手需要获得权限后提交相关的 Flag 值。

比赛内容包括应用安全、操作系统安全、逆向、Web 安全、数据安全、应急响应、蜜罐、物联网安全、PWN、恶意代码、系统安全、数据库安全、中间件安全、密码技术、数据恢复、计算机取证、 工控网

络安全以及等级保护 2.0 相关技术要求等。

计分方式与复赛 CTF 夺旗赛一致。

三、技术平台

（一）初赛平台介绍

竞赛平台采用虚拟化的形式进行运作，底层采用了虚拟化技术进行配置，在平台中对 Web 安全问题、二进制安全问题、逆向安全问题、移动安全问题、数据安全问题、5G 安全问题、区块链安全问题，提供模拟环境及演练模拟试题。平台整体架构包含比赛管理员配置页面、比赛用户答题页面及虚拟化场景建设节点。参赛选手可通过 Web 页面进行访问，查看到已经开放的赛题信息。

（二）复赛及决赛平台介绍

1)平台简介

竞赛平台采用虚拟化的形式进行运作，底层采用了 python+docker 的虚拟化技术进行配置，在平台中对 Web 安全问题、二进制安全问题、逆向安全问题、移动安全问题、数据安全问题、5G 安全问题、区块链安全问题，提供模拟环境及演练模拟试题，所有参赛选手均采用独立环境进行运营，保障在网络上的隔离确保运行环境的安全。平台整体架构包含比赛管理员配置页面、比赛用户答题页面

及虚拟化场景建设节点。参赛选手可通过 Web 页面进行访问，查看到已经开放的赛题信息及比赛事实运行情况。竞赛现场配备大屏实时展示比赛进展。

2)系统结构及部署

系统服务组件主要有支持 Web 访问的 Nginx 服务、用来支撑数据存储调用的 mysql 数据库，缓解数据库调用压力的 redis 组件服务组成。在部署架构上系统是在服务器上搭建虚拟环境，各服务组件再通过虚拟环境下的系统进行集成化部署。

3)网络架构

赛场网络分为：参赛选手 IP 段，服务器 IP 段，管理员 IP 段，所有参赛选手的 IP 段不能互相访问。所有参赛选手都可以访问到服务段开放的端口，管理员 IP 段可以访问所有段。上述网络环境通过划分 Vlan 后再由三层防火墙进行网络隔离后实现。

4)高可用配置

系统多机负载均衡主要利用 Nginx 服务，在 Nginx 服务配置中添加多机的 IP 地址与端口，基于转发策略对平台的访问流量进行目的转发，分发到系统下对应的主机，实现数据请求。

（三）题目部署

题目部署依托于线上的虚拟环境，专家组将题目运行环境进行打包，打包完成后由竞赛组委会统一上传至竞赛平台。

（四）应急响应及灾备

1.数据备份

系统通过多机部署搭建一个虚拟环境，在这个环境下模拟部署多台服务主机部署，通过 keeplived 组件定义主服务器与备份服务器，在主服务器和备份服务器上面部署相同的服务配置，使用一个虚拟 IP 地址对外提供服务，当主服务器出现故障时，虚拟 IP 地址会自动漂移到备份服务器。通过 keeplived 组件保障数据的实时备份，其形式可以是主从模式，实现数据双机热备；也可以是主主模式，实现数据双机互备。

2.灾难恢复

本次比赛采用数据库实时导出方式进行数据备份，通过实时数据备份的方式实时将备份文件拷贝至运维终端，在发生服务器故障时临时开启云虚拟环境对数据进行恢复及再开赛等工作。

3.比赛稳定性保证

比赛期间配备专门的平台运维团队，提供技术咨询，以保障平台的稳定运行。

四、竞赛需知

（一）疫情安全保障

复赛及决赛竞赛签到时，所有人员须持有“健康码”绿码及 14 天内未前往中高风险地区手机行程轨迹证明，来自高风险地区人员还需持 7 日内核酸检测结果为阴性的报告，接受现场体温检测，符合防疫要求后方可进入活动地点。体温在 37.3 摄氏度及以上人员、发热和咳嗽等症状人员不得进入，同时立即报告并按要求安排就医。

（二）竞赛注意事项及规则

1、参赛选手需自已提前准备工具。

2、复赛及决赛参赛选手须自带电脑、有线鼠标、网络安全类软件工具进入考场，赛场不负责自带物品的检修和排故。

3、复赛及决赛现场仅提供网线接入方式，参赛选手需自带 RJ45 网线转接器。

4、建议参赛选手全程采用 chrome、firefox 浏览器进行访问，不能使用隐私模式访问平台，可能造成平台无法访问，答题异常等情况。

5、禁止参赛选手之间互相共享登陆账号，或将账号共享给其他无关人员。

6、禁止任何参赛选手合作解题，或者共享 flag、hint、解题思路等任何比赛相关信息。

7、禁止攻击比赛平台，如果发现平台漏洞，请立刻向组委会报告。

8、禁止向比赛平台发送大流量、比赛题目不需要使用的扫描器。

9、禁止对提交的 flag 进行爆破。

10、复赛及决赛期间禁止参赛选手使用任何方式连入互联网。

11、禁止对现场网络环境进行破坏。

12、复赛及决赛中所有参赛选手将被分配到不同的环境，禁止访问他人环境。

13、参赛选手如有任何违反本注意事项禁止的行为及其他违规行为，现场裁判将会视情况予以警告，扣分或者取消比赛资格，并全场公告。

14、比赛过程中，参赛选手请遵守工作人员指示，尊重裁判裁决。

15、大赛组委会拥有对赛题、规则等一切事项的最终解释权。

五、附件：竞赛大纲

（一）政策法规和标准

熟悉《中华人民共和国网络安全法》的相关内容。掌握安全法所涉及的角色、应当履行的法律责任与义务。掌握网络安全法在学习、宣传和贯彻实施中所涉及的内容。熟悉《中华人民共和国密码法》的相关内容。掌握密码法所涉及的内容，尤其是责任与义务。熟悉《网络安全审查办法》《关于推进国家技术创新中心建设的总体方案》等

国家信息技术应用创新的相关法规条 例。了解《中华人民共和国数据安全法》内容。熟悉《国家网络安全事件应急预案》相关内容。熟悉网 络安全事件的产生原因、目的、分级，了解网络安全应急事件处置组织机构与各部门相关职责，以及针对检测与预警的响应措施等。熟悉网络等级保护定级范围、评审要求、备案等政策要求；了解网络单元安全防护定级方法、定级对象命名规则、定级报告内容、定级备案等相关信息。了解安全风险评估工作的国际标准名称（ISO/IEC TR 13335、ISO/IEC17799、ISO/IEC 27001 等），了解《信息系统安全等级保护定级指南》《信息系统安全等级保护实施指南》等国家标准总体情况。了解《中华人民共和国计算机信息系统安全保护条例》《关键信息基础设施安全保护条例》等相关国家网络安全法律规范条例。

（二）风险评估

掌握常规的渗透测试技术。熟练使用各种常见渗透测试工具，渗透测试技术包括：踩点扫描探测、信息收集、暴力破解、常规漏洞利用、Web 权限获取、提权、溢出攻击、植入后门、内网渗透等。掌握常见安全漏洞的代码审计和代码加固技术，常见漏洞至少包括：缓冲区溢出、拒绝服务、远程命令执行、注入、跨站、Web 提权。

（三）物联网安全

掌握常规的物联网安全分析技术,包括但不限于:二进制固件提取技术,物联网固件分析技术,物联网协议分析,物联网设备架构分析。

熟练掌握 arm/mips 等架构下的二进制逆向技术。

（四）应急响应

掌握应急响应相关技术，包括：入侵取证分析、日志审计分析等。了解操作系统（Windows、Linux 等）的常规安全防护技术。能熟练利用系统日志、应用程序日志等溯源攻击途径；掌握系统账号、文件系统、网络参数、服务、日志审计等项目的安全检测与安全加固方法。

（五）信创

了解信创相关操作系统、数据库、中间件和安全产品。掌握对信创产品的安全测试和漏洞挖掘技术。

（六）其他

熟悉密码技术的概念、加密体制的分类、常见加密方式、 密码协议与密码分析工具的利用；

掌握 CTF 五个知识点的分析利用；

熟悉物联网、工业控制、无线、网络设备等相关方面的安全问题；

熟悉移动互联网恶意程序监测与处置机制，掌握移动应用的逆向分析和代码审计技术、移动应用的安全防护方法等；

掌握常见协议分析工具的使用，常见数据包分析方法；

熟练使用数据恢复的常用技术等相关知识点内容；

熟悉恶意代码的识别方法及防护措施。能运用相关技术发现、隔离、清除常见恶意代码；并能对常见恶意代码进行逆向分析。