2023年“湖北工匠杯”技能大赛——湖北

省第三届信息通信网络运行管理员

（网络信息安全）职业技能

竞赛实施方案

湖北省通信管理局

2023年10月

目 录

一、赛事级别 2

二、赛制说明 2

（一）预赛 2

（二）决赛 2

三、竞赛大纲 5

（一）法律法规和标准 6

（二）风险评估 6

（三）安全防护 6

（四）应急响应 7

（五）安全加固 7

（六）数据安全 7

（七）物联网安全 8

（八）其他 8

四、竞赛时间安排 8

五、竞赛奖项设置 9

六、参赛人员守则 9

七、注意事项 11

# 一、赛事级别

本次赛事是经省人力资源和社会保障厅批准的省级一类大赛，由湖北省通信管理局、湖北省人力资源和社会保障厅、湖北省总工会、湖北省人民政府国有资产监督管理委员会主办；湖北通信行业职业技能鉴定中心、湖北省通信行业协会、湖北省互联网协会承办；中国联合网络通信有限公司湖北省分公司协办，智网安云信息技术股份有限公司支撑，湖北省邮电学校具体实施。

组委会将根据本次比赛结果，推荐排名靠前的选手参加“2023年第四届全国电信和互联网行业职业技能竞赛（网络与信息安全管理员——通信网络安全方向）暨第十二届信息通信网络安全管理员职业技能竞赛”全国总决赛。

# 二、赛制说明

为切实提升参赛单位的信息安全保障能力，检验参赛人员的信息安全综合能力，本次大赛预赛为各参赛企业自行组织，决赛将采用理论赛、CTF(夺旗赛)、AWD(网络攻防对抗赛）三种模式展开,均线下进行，具体说明如下：

### （一）预赛

由各参赛企业自行组织。根据各单位自行组织的预赛比赛成绩排名，按决赛报名要求推荐排名靠前的选手报名参加决赛。各单位自行组织的预赛成绩不计入决赛成绩。

（二）决赛

决赛分为个人赛和团队赛，全部为线下进行。

1．个人赛分为理论知识考试及CTF（夺旗赛）

（1）个人理论知识考试，采用线下答题方式；

（2）个人CTF（夺旗赛）采用动态计分叠加一血奖励积分方式，考试时长为3小时,共10～12道考题，通过离线分析或在线技术研究的方式夺旗，技术类型覆盖Web渗透、二进制漏洞挖掘利用、密码分析、取证分析、逆向分析、安全编程等网络安全各项技术，提交验证正确后给予相应分数。

（3）个人赛总分计算：个人总分=理论考试得分\*20%+个人CTF（夺旗赛）得分\*80% （最后均折算成百分制再累加。）

2．团队赛分为AWD及现场知识问答

（1）AWD（网络攻防赛）考试时长为3小时，每个参赛队伍拥有3～4个攻防环境，开赛时同时开启，防守机存在若干安全漏洞，每支队伍可使用普通用户权限登录本队防守机进行加固，加固动作不得影响正常服务运行和功能使用，并在规定时间内充分挖掘环境漏洞并利用，通过修补自身防守机的漏洞进行防御以免失分，同时在竞赛网络空间中攻击其他队伍的环境，尝试获取其他所有队伍防守机的权限。参赛队伍通过离线代码分析、Web渗透测试、二进制漏洞挖掘等技术对其余参赛队伍的攻防环境发起攻击并获得Flag，提交验证正确后给予相应分数，同时需要维护参赛队伍自身攻防环境安全与稳定，若被其他参赛队伍获得Flag或者攻防环境无法正常运行，平台会对其进行扣分。提交本队核心Flag值不得分；成功提交其他队伍的Flag得分。

（2）团队现场知识问答时长为2小时，由AWD（网络攻防赛）决胜出的前8支队伍，共计24名选手参加知识问答进行现场比拼，角逐团队最终排名。答题题目均为专业知识问答。

（3）团队赛总分计算：团队总分=AWD（网络攻防赛）赛得分\*80%+现场知识问答得分\*20% （最后均折算成百分制再累加。）

3．决赛计分规则

（1）个人理论成绩以百分制计分。

（2）个人CTF（夺旗赛）计分规则采取动态计分+一血奖励机制进行统计分数。

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。本次比赛最高分为1000分。

一血奖励机制附加在动态计分方式中同步进行。默认一血奖励比例为：

第一名:题目分值\*10%；

第二名:题目分值\*5%；

第三名:题目分值\*3%。

（3）AWD计分规则—团队决赛计分规则

每个参赛队伍基础分均为5000分，平台根据比赛轮次刷新攻防环境中的Flag值，轮次时长20分钟，轮次Flag分值50分，每次轮次结束后，平台会根据上一轮次参赛队伍的答题情况进行计分。通过最终排行榜成绩计算本轮竞赛排名。

比赛过程中，不得停止本队防守机的服务和关键页面功能，系统不定时检测，如果检测到任何1支队伍服务宕机（端口、Webflag标志文件无法访问），无论任何原因导致，每次扣所属队伍100分。每支队伍可申请重置服务器到初始状态，每次重置扣500 分。比赛过程中，裁判可抽查得分点的方法，疑似非法手段获取的，取消该项得分，情节严重者取消成绩。

总分=初始分+对抗得分-对抗失分-异常扣分-重置扣分，在规定时间内总分最高的队伍获胜，得分一致则用时最短者获胜。

（4）团队现场知识问答—团队决赛计分规则

* 必答题16题，参赛队推选代表答题，每队答2题，每题20分，回答正确加10分，回答错误不计分；
* 抢答题16题，每题10分，回答正确加10分，回答错误及抢答犯规均扣5分；
* 风险题48题，分值为20分、30分、40分的题型各16题，每队派选手作答（每队每人限选1题）回答正确获得对应加分，回答错误扣除对应分值。
* 如在现场知识问答环节出现比分相同的情况，则进行加时赛，以加时赛正确答题数量多的队伍胜出为原则。

三、竞赛大纲

熟悉我国网络和数据安全领域相关法律法规，结合近年来发生的网络和数据安全问题和事件，聚焦典型安全漏洞和攻防场景；围绕定级备案、监测预警、漏洞挖掘、风险评估、安全运维、团队协助、安全加固和应急响应等方面，在综合竞赛环境中实现业务场景建模；重点考察选手对网络空间安全的综合攻防能力和在安全工作岗位的技术水平和运维能力。
 （一）法律法规和标准

《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》、《通信网络安全防护管理办法》、《国家网络安全事件应急预案》、《工业和信息化领域数据安全管理办法（试行）》、《公共互联网网络安全威胁监测与处置办法》、ISO/IEC 27001等。

（二）风险评估

掌握常规的渗透测试技术及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）安全防护

熟悉中间件和 Web 应用的安全检测与防护方法。

了解主流厂商网络设备的调试与配置。

了解主流数据库系统的补丁、账号管理、口令强度、有效期检查、远程服务、存储过程、审核层次、备份过程、用户功能和权限控制等基础技术。

掌握主机操作系统和应用软件的安全配置、主机运行的应用程序、正常运行所必需的端口、服务的正确配置。

掌握文件系统、关键数据、配置信息、口令、用户权限等内容的完整性备份。

（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、流量审计分析等。

了解操作系统（Windows、Linux、Unix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。

熟悉常见网络设备和安全设备的功能及使用方法。包括：路由器、交换机、防火墙（含 Web 应用防火墙）、入侵检测系统、抗拒绝服务攻击系统、网页防篡改系统、漏洞扫描系统等。

（五）安全加固

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。

熟悉Web cms、中间件、数据库等常用Web应用的加固知识，并熟练应用防火墙、IPS、IDS等安全设备进行辅助加固措施。

（六）数据安全

了解云计算和大数据的基本概念及特征，了解云计算和大数据技术带来的安全问题。包括：虚拟机安全、应用程序安全、数据安全；了解利用大数据分析技术提升网络系统安全隐患发现和防护能力。

（七）物联网安全

了解物联网的基本概念及相关基础技术，了解ID/IC卡的安全漏洞检测和发现技术，了解智能卡常见加解密算法。了解物联网应用环境中典型的安全攻击，如RFID攻击等。

（八）其他

了解密码学的概念、加密体制的分类、常见加密方式与密码分析工具的利用。

掌握隐写术在不同场景下的具体使用。

掌握网络攻击原理与常见网络攻击协议。

掌握常见 Web 攻击种类，常见的 Web 利用方式。

掌握注入攻击的类型，注入攻击利用的方式。

熟练掌握漏洞产生原因、漏洞的利用与漏洞防护方式。

熟练掌握恶意代码与逆向技术的常用工具与具体使用方法。

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。

四、竞赛时间安排

|  |  |
| --- | --- |
| 日期 | 内容 |
| 2023年10月20日-30日 | 竞赛报名 |
| 2023年10月31日 | 报名审核 |
| 2023年11月8日-9日 | 线下决赛 |

# 五、竞赛奖项设置

团队（按参赛团队AWD（网络攻防赛）及团队现场知识问答综合得分排名评奖）设一等奖1名；二等奖2名；三等奖5名。

个人（按个人理论考试成绩+CTF比赛成绩总分评奖）得分1-3名，颁发“个人一等奖”证书，并按程序申报“湖北省技术能手”；个人得分第4-8名，颁发“个人二等奖”证书，并按程序可晋升高级工职业资格或职业技能等级，已具有高级工职业资格或职业技能等级的，可晋升技师职业资格或职业技能等级；个人得分第9-15名，颁发“个人三等奖”证书。

团队排名前8名的战队带队老师授予本次比赛“优秀指导老师”称号。

对贡献突出的承办、协办单位和技术支持单位，由竞赛组委会颁发“突出贡献奖”奖牌和荣誉证书。

# 六、参赛人员守则

（一）参赛队伍须凭有效身份证件及参赛证进入赛场。

（二）参赛队伍自行携带笔记本电脑、鼠标、键盘、网线扩展坞进入赛场，提前准备相关工具。

（三）比赛期间，现场不提供互联网上网环境，参赛选手不得通过无线上网卡等设备将比赛网络环境接入互联网，严禁携带、使用手机、蓝牙等任何可远程通讯的设备。

（四）严禁干扰他人比赛，尤其是通过技术手段对上机操作环境进行攻击，比赛过程中严禁参赛队伍向比赛服务器、参赛队伍主机等设施发起任何可能影响比赛正常进行的攻击或恶意操作（比如暴力破解、CC/DDoS/ARP等），如有发现，裁判组将给予扣分，严重者将被禁止比赛，分数记0分。

（五）比赛过程中禁止使用通用防御脚本/工具防御对手攻击，一旦被检测并查实使用通用防御则进行扣分并警告；经警告3次仍然不撤销通用防御的队伍，决赛记0分。

（六）禁止对赛题服务所在环境进行权限提升，禁止利用已获得的账户权限对Flag值等比赛关键数据进行修改，如有发现将被禁止比赛，分数记0分。

（七）参赛队伍在比赛期间需遵循裁判及现场工作人员的安排，如有疑问请举手示意。

（八）参赛队伍未经裁判同意，禁止进入他人赛位，干扰其他队伍比赛。

（九）遵守大赛纪律，切勿喧哗，服从裁判，不得对他人进行语言或人身攻击。比赛过程中，不同队伍之间不允许以任何形式相互讨论、交流、合作、分享资料，一经发现直接取消比赛资格，相关队伍立刻离场。

（十）比赛过程中以及比赛结束后裁判有权抽查队伍解题方法/得分思路，如果发现回答有误，疑似通过作弊获得分数将对队伍扣分，严重者取消队伍参赛资格。

（十一）在攻防环节开始后，一切由比赛选手造成的赛题服务器异常问题，裁判均不予处理，异常服务器所属队伍按规则失去相应分数，除非出现网络连接异常通信故障（网线、公共核心交换）。

（十二）违反上述规定者，现场裁判组将视情给予口头警告、扣分、取消参赛资格等处罚。

# 七、注意事项

（一）各参赛选手需自带笔记本电脑、鼠标、键盘、网线扩展坞。选手登录竞赛系统后，由竞赛系统引导进入竞赛环境。

（二）攻击只针对对方的服务器区，禁止对其他网络设备进行攻击。

（三）禁止使用DDoS攻击、局域网攻击工具。

（四）在竞赛进行期间，竞赛场地内将开启信号干扰器，屏蔽现场的手机信号和WLAN信号等。