2022年首届湖北省大学生信创大赛决赛
技术文件

“奇安信杯”决赛赛项

湖北省高等教育学会

奇安信科技集团股份有限公司

2022年04月

目录

1.项目简介

1.1 项目描述

赛项名称：“奇安信杯”网络安全赛道（决赛）

比赛时间： 2022 年 5 月 21 日

为深入贯彻落实习近平总书记关于建设网络强国的重要论述和党中央、国务院关于建设网络强国、数字中国、智慧社会的战略部署，培养信息技术应用创新领域特殊人才，增强师生自主创新意识，提升各高校信息技术创新、网络空间安全能力，本届大赛由湖北省经信厅指导，湖北省高等教育学会主办，武汉职业技术学院承办，奇安信科技集团股份有限公司等协办。

1.2 竞赛目的

通过赛项检验参赛选手按照等保要求加固网络、安全架构、网络安全运维、渗透测试技术等能力，检验参赛队计划组织和团队协作等综合职业素养，培养学生创新能力和实践动手能力，提升学生职业能力和就业竞争力。通过竞赛引领专业教学改革，丰富完善学习领域课程建设，使人才培养更贴近岗位实际，实现以赛促教、以赛促学、以赛促改的产教融合格局，提升专业培养服务社会和行业发展的能力，为国家信息安全行业培养选拔技术技能型人才。

2.选手应具备的能力

模块	能力描述
决赛	**攻防混战**
	• 个人需要知道和理解： • 网络威胁行为者,他们的技术和他们的方法 • 用于检测各种可利用的活动的方法和技术 • 网络情报和信息收集能力 • 网络威胁和漏洞 • 网络安全基础知识(例如加密、防火墙、认证、诱捕系统、外围保护) • 漏洞信息传播源(例如警报、通知、勘误) • 哪些系统文件(如日志文件、注册表文件、配置文件)包含相关信

	息以及在何处查找这些系统文件 • 开发工具的结构、方法和策略(例如嗅探、记录键盘)和技术(例如获取后门访问、收集机密数据、对网络中的其他系统进行漏洞分析) • 预测、模拟威胁能力和行动的内部策略 • 内部和外部合作伙伴的网络操作能力和工具使用能力 • 目标开发(即概念、角色、责任、产品等) • 系统开发过程遗留物和司法鉴定应用案例
	• 个人应能够：掌握相关技术 • 网络协议分析 • Web 攻击 • Web 日志审计与分析 • 路由器漏洞利用 • ACM 编程 • 各种环境的取证分析 • 二进制程序的逆向分析，二进制程序的漏洞挖掘与利用，操作系统内和安全。

3.竞赛概述

3.1 竞赛时长

决赛预计时长 180 分钟，采购攻防混战的比赛形式，如选手决赛成绩出现同分情况的，按照先后顺序计算排名顺序。

3.2 决赛简述

攻防混战考察选手在安全攻击与安全防守方面的技能。要求选手在规定保护时间内对各自的靶机进行安全加固;过了保护时间即进入混战阶段，各战队可对其他战队靶机开展自由攻击并获取对应分值。

3.3 命题方案

本赛项命题、赛题结构及设计由奇安信高校合作中心进行命题，采用国内常用的攻防混战，即 AWD 模式开展比赛。

攻防对抗阶段需要选手在防守自己的服务器的同时，要找到其他选手所防护服务器中的脆弱点，对其进行攻击，目的是攻破对方的主机，获取存在于对方服务器上的 flag 值，另一方面要加固自己服务器上的脆弱点，防止其他选手攻破自己的服务器后获取自己的 flag 值。攻击时考察的知识点和综合渗透基本一致，但防守时需要选手对服务器中的脆弱点有更深层次的了解，因为需要对发现的脆

弱点进行修复，包括配置的修改，代码的修改，关闭不必要的端口等操作。

4. 评分规则

4.1 裁判组构成

1. 裁判长：由命题组组长担任，执行裁判长负责制。

2. 裁判员：根据情况，各参赛学校可选派一名专业教师担任裁判员。

4.2 计分规则

（1） 动态 flag 时间设置

假设平台设定每轮的用时为 10 分钟（实际视情况而定），则每 10 分钟 flag 更新一次。随着比赛进行，攻防比赛的后半部分每轮的时间会变短，需要更精细的控制各个时间段的刷新时间。

获取 flag 一般是从被攻击者的机器上请求 flag 机器，或执行服务器上特定的程序。

（2） 计分模式

分数不设上限，每个队伍拿到 flag 即可获得固定分数，服务判 down 则会丢固定分数，队伍分数为 0 攻击此队伍也可继续得分。

（3） 服务状态检测

比赛过程中每轮都要检测所有选手服务的状态，防止选手暴力删除服务，check 脚本可以选择由外部 check 机器检测，也可以下发到选手服务器中执行，下发到服务器中可以检测更多的参数。一般检测时间是一轮中。

5. 项目特别规定

（4） 扰乱赛场秩序，干扰裁判员工作，视情节扣分，情况严重者取消比赛资格。

- 比赛过程中禁止对比赛平台进行攻击，一经发现取消比赛资格。
- 禁止对“规定 iP”以外的地址进行攻击，禁止对比赛平台进行攻击
- 网络设备已配置安全策略及日志记录和告警功能;对网络设备和竞技平台的扫描或渗透都会被记录和告警，一经发现攻击行为，安全策略

会阻断流量，上报裁判长按规程处理。

（5） 系统自动启动违规检测，如有如下违规行为，给予扣分：

- 发现 FLAG 异常（譬如：删除、修改、杀进程等）；
- 关闭赛卷中要求开启的端口；
- 自行改动攻防阶段靶机的 IP 参数；
- 靶机关闭。

7.健康和安全

（1）赛场人员安全要求

1）现场裁判、选手、工作人员在竞赛期间应该遵守主办方的安全规定和要求;

2）参赛选手进入竞赛场地后，须听从并尊重裁判人员的管理，文明参赛;

3）参赛选手必须在确保人身安全和设备安全的前提下开始竞赛，发现或发生有关安全问题，应立即向裁判报告;

4）参赛选手严禁在赛场区域内吸烟和私自动用明火，严禁携带易燃易爆物品。

（2）场地设备安全要求

1）设施设备安全操作要求

A. 禁止选手及所有参加赛事的人员携带任何有毒有害物品进入竞赛现场。

B. 赛点单位应设置专门的安全防卫组，负责竞赛期间健康和安全事务。主要包括检查竞赛场地、与会人员居住地、车辆交通及其周围环境的安全防卫；制定紧急应对方案；监督与会人员食品安全与卫生；分析和处理安全突发事件等工作。

C. 赛场须配备相应医务人员，并备有相应急救设施。

2）赛场消防安全要求

A. 消防设施、器材和消防安全标志全都在位且功能完整。

B. 消防安全重点部位人员正常在岗工作。

3）安全标识张贴要求

安全出口、疏散通道保证畅通，安全疏散指示标志、应急照明完好无损，竞

赛场地安全疏散通道禁止被占用。

4）设备安全操作规程

A. 禁止带电进行线路拆改工作。

B. 所有修改必须在停机状态下进行。

C. 在进行任何安装或维修工作前，必须确认设备处于停止状态。

（3）疫情防控要求

1）根据国家及当地疫情防控的相关规定，做好赛前集中技术工作对接、比赛报到、住宿、交通，以及赛场人流控制、核酸检测、体温检测等环节的相关防疫工作。如体温检测≥37.3℃，引导至所设临时隔离等候区域，参赛人员暂停竞赛活动并马上报告主办方，按照疫情防控处置流程将发热人员送至就近指定医疗机构的发热门诊就诊。如医疗机构确定其无问题可返回参赛（受此影响的竞赛时间不补）。

2）任何参赛选手和其他人员须遵照执行防疫工作相关措施要求，如：全程佩戴口罩、保持安全距离；防疫物品自备，一次性医用口罩使用完毕后，须丢弃到专用垃圾桶。

8.开放赛场

（一）在竞赛过程中，借鉴世界技能大赛组织方式，尝试开放式竞赛方式，广泛宣传，积极组织院校师生、企业员工等人员进行现场观摩，营造参与技能学习、实现技能成才的氛围。

1）赛场内除指定的裁判、工作人员外，其他与会人员须经主办方同意或在主办方负责人陪同下，佩带相应的标志方可进入赛场内；

2）允许进入赛场的人员，只可在参观通道内观摩竞赛，不得使用录像设备长时间拍摄选手工位、屏幕；

3）允许进入赛场的人员应遵守赛场规则，不得与选手交谈，不得妨碍、干扰选手竞赛；

4）允许进入赛场的人员不得在场内吸烟、喧哗；

（二）如疫情防控要求，不能进入赛场进行公开观摩，采用视频观看方式。

1）视频观摩

赛场外设置开放式观摩区，向媒体、企业代表、院校师生等社会公众开放，通过大屏幕对赛场进行直播，同时还可以通过竞赛系统进度监控图实时观看选手答题进度。

2）组织安排

在竞赛开始 30 分钟之后，由承办校组织并派人带领媒体、专家、企业代表、院校师生等进入赛场外的开放式观摩区，按照指定路线进行观摩。

3）纪律要求

为保证大赛顺利进行，在观摩期间应遵循以下纪律要求：

1. 除与竞赛直接有关工作人员、裁判员、参赛选手外，其余人员均为观摩观众。

2. 不得违反职大赛规定的各项纪律。

3. 观摩人员需批准，佩戴观摩证件，遵循观摩区的工作人员指挥。

4. 文明观摩，保持观摩区清洁，不得大声喧哗，杜绝各种违反观摩秩序的不文明行为。

9.绿色环保

（一）环境保护

环境整洁卫生，体现绿色环保，严格遵守竞赛规则，提高安全意识和卫生意识，按照要求穿戴工作服装、安全鞋、手套、安全眼镜、耳塞等劳保用品，严格遵守职业规范。

所有竞赛相关人员必须保持场地整洁。交通路线、走廊、楼梯、紧急疏散通道、灭火器及其他救生设备周边必须保持畅通无障碍，竞赛结束后，选手要整理好竞赛工位的卫生，赛场保洁人员要保障赛场整体的环境卫生，体现安全、整洁、有序，将垃圾分类处理。

将废弃物降至最低水平，多余废弃的耗材等要放入到指定垃圾桶内。

（二）可持续性

竞赛项目设计和筹备工作要遵循可持续发展原则，耗材回收有序，设备循环使用。工位将被用于与技能相对应的模块进行测试。

为了减少网络设备的数量，工位设备将用于多个模块的测试环境，使用技

术手段进行快速轮替，以免造成浪费。