

2022 第三届“网鼎杯”网络安全大赛半决赛、总决赛

赛制介绍

依照《2022年第三届“网鼎杯”网络安全大赛规则》，半决赛及总决赛采用多种赛制融合的竞赛模式，时长均为8小时，半决赛比赛时间为4月14日10:00-18:00，总决赛比赛时间为4月15日9:00-17:00。

半决赛各分组内排名前12的战队，以及在剩余战队中总积分靠前的2支战队，共计50支晋级总决赛。总决赛不再分组，按照比赛得分由高至低确认最终排名。

一、半决赛赛制

半决赛采用“共同防御+实景防御(RDG)+人工智能漏洞挖掘(RHG)+突破+云境靶场挑战”等多种赛制相融合的竞技方式。

其中“共同防御”场景中新增“情报共享平台”，借鉴网络攻击的热点事件设计场景，参与演练的各界参赛选手协同联动，共同应对网络安全威胁。

赛制	时间	赛制描述
共同防御	10:00-11:40	通过仿真基础设施运营单位内部通信网络业务场景，构建任务剧情。题目会以场景中的某些

		<p>任务的形式存在。参赛选手需要按照对剧情的理解，找到业务场景中的防御任务，进行威胁发现、漏洞修复、网络配置加固、攻击溯源等操作。并在探索、完成任务过程中，及时将有效的情报通过共同防御协同平台分享出来。最终通过共同的力量把安全事件消除清零，并整合力量形成共同防御协同联动的机制。</p>
<p>实景防御 (RDG)</p>	<p>14:00-18:00</p>	<p>每支队伍提供一台虚拟机，该虚拟机中放置若干个带有漏洞的Docker容器，选手需要SSH登录虚拟机，通过Docker命令发现容器中的预置漏洞，并设计用于漏洞的修补包（xx.tar.gz），包内需要包含一个update.sh的可执行文件，在平台上传修补包并申请防御判定，按轮次得分，综合考核选手的网络配置、漏洞发现、漏洞修复能力等。</p>
<p>人工智能</p>	<p>10:00-18:00</p>	<p>靶标由带有漏洞的二进制文</p>

<p>漏洞挖掘 (RHG)</p>		<p>件构成，选手可以自行开发人工智能“机器人”，并通过平台提供的接口自动获取题目、分析题目、挖掘漏洞利用、获取靶标flag并提交这一系列操作。RHG阶段选手可自行调试“机器人”，人机配合帮助“机器人”答题。</p> <p>1、测试时间为10:00-13:00，测试阶段将开启1道测试题，该阶段不得分。</p> <p>2、挑战时间为13:00-18:00，将开启9道题目。</p>
<p>突破</p>	<p>10:00-13:00</p>	<p>采用网络夺旗形式，题目将以预设了漏洞的仿真环境形式下发。参赛队通过找到题目环境中的flag（有特定格式的字符串，详见参赛手册）后提交得分。</p>
<p>云境靶场 挑战</p>	<p>16:00-18:00</p>	<p>在平行仿真的云境靶场——网鼎之城中设置了一套由多个网络节点组成的仿真场景。</p> <p>进入云境的战队在靶场漫游时，制定渗透路径，获取更高权</p>

		<p>限或发现更严重漏洞并进行利用，以找到flag提交，在平台验证成功后可获得相应分数。</p> <p>于15:30确定云境靶场挑战入围名单，原则上由每个分组积分榜排名前20的队伍组成，共计80支，裁判组会视现场答题情况调整进入云境靶场挑战的资格。</p>
--	--	--

二、总决赛赛制

总决赛依旧采用多种赛制相融合的竞技方式，晋级选手将不再分组，各队选手共同角逐网鼎杯最高荣誉。

赛制	时间	赛制描述
突破	09:00-13:00	<p>比赛设置若干个仿真场景，选手需要对仿真场景中的预置漏洞进行利用，拿到flag值在平台提交，按轮次得分，综合考核选手的漏洞挖掘、漏洞利用能力等。</p>
实景防御 (RDG)	13:00-17:00	<p>每支队伍提供一台虚拟机，该虚拟机中放置若干个带有漏洞的Docker容器，选手需</p>

		<p>要 SSH 登录虚拟机，通过 Docker 命令发现容器中的预置漏洞，并设计用于漏洞的修补包 (xx.tar.gz)，包内需要包含一个 update.sh 的可执行文件，在平台上传修补包并申请防御判定，按轮次得分，综合考核选手的网络配置、漏洞发现、漏洞修复能力等。</p>
<p>共同防御</p>	<p>14:00-17:00</p>	<p>模式同半决赛共同防御环节，剧情将设定在大型城市级工业生产场景下的安全威胁及共同应对。参赛选手需要通过一系列协同防御的任务，完成对城市工业网络恶意安全威胁行为的防范及反制，构建网络空间安全责任共同体。通过一系列协同防御的任务，完成对关键行业恶意网络威胁行为的防范及反制，构建网络空间安全责任共同体。</p>
<p>云境靶场挑战</p>	<p>09:00-17:00</p>	<p>开放8小时，所有进入总决</p>

		赛的队伍均可挑战。
--	--	-----------

三、积分模式

半决赛和总决赛积分模式如下：

半决赛	
共同防御	沙漏积分
突破	
云境靶场挑战	固定积分
人工智能漏洞挖掘 (RHG)	排名积分
实景防御 (RDG)	轮次积分
总决赛	
共同防御	沙漏积分
云境靶场挑战	固定积分
突破	轮次积分
实景防御 (RDG)	

沙漏积分：当某题目被选手第一次正确解答后，其题目分值每经过n分钟将下降m分，题目分值的下降不影响前面正确解答者，题目分值下降到50分将不再下降。

名次排名：RHG排名分为5个档：1-10名、11-30名、31-50名、51-100名、101-500名。同个档内得分一致。

轮次积分：每20分钟为一轮，每轮比赛题目积分随攻守格局变化而改变，每轮次内有效的攻击和防御都会分别计分，服务异常不扣分。

情报共享平台：共同防御环节，每一道题目正确解答者均可分享情报，但只有分享情报合格者前20名才可获得该环节得分。

最终成绩取各部分分数总和，按由高至低排列，分数相同情况下，以靶场最终得分的时间先后顺序排序，用时短者排名高于用时较长者。

四、其他规则

1、比赛当天所有参赛选手需持身份证原件到达比赛现场，迟到超半小时禁止入场。

2、裁判有权根据现场情况对违规、违纪战队进行减分处理。

3、比赛过程中请随时关注答题页面的公告栏，所有执行规则及判罚以最新公告为准。

4、比赛过程中对平台或题目有问题，可以在答题页面端点击“呼叫裁判”按钮反馈问题，请描述清楚遇到的问题，否则可能影响应答效率。禁止随意在场内走动。

5、为维护现场秩序，避免跨战队交流，去洗手间请举手示意，经过工作人员确认后可以从相应出口有序去洗手间。