

2020年第二届“网鼎杯”网络安全大赛线下赛

赛制细则

按照《2020年第二届“网鼎杯”网络安全大赛规则》，大赛半决赛及总决赛采用AWD PLUS攻防兼备+靶场演练赛制，比赛时间为10:00-18:00，时长8小时。

半决赛开赛后，先进行AWD PLUS攻防兼备模式，攻击和防守成功都会得分。靶场全天共开放2次，每次开放2个小时，开放时间为13:00-15:00、16:00-18:00，具体参见靶场环节说明。

总决赛全天同时进行AWD PLUS攻防兼备模式和靶场演练模式，参赛战队可以自由选择挑战目标和得分策略。

半决赛、总决赛比赛成绩为每场AWD PLUS模式+靶场模式得分（归一化之后）加权之和。

半决赛各个分组组内排名前12的战队，以及在剩下的队伍中靶场分靠前的2个队伍，合计50队晋级总决赛。总决赛按照得分高低排名并确定一二三等奖。

一、线下赛赛制

线下赛分为半决赛和决赛，均为采用AWD PLUS攻防兼备+靶场演练赛制的团队赛，比赛时间为10:00-18:00，时长8小时，战队内所有队员共享一套题目和场景环境，和其他战队间不互享，比赛过程中，战队中任何队员得分都会计入战队总分。开赛后攻防兼备及靶场演练模式的

靶标同时上线，其中半决赛阶段，所有选手需要在AWD PLUS攻防兼备模式中获取积分，然后在比赛赛程中，分别有两个时间段会为每组积分排在前列的战队开放靶场演练通道，有机会进入靶场演练模式的战队将同时进行AWD PLUS攻防及靶场挑战。总决赛阶段AWD PLUS模式和靶场模式面向所有战队全程同时开放。在无裁判加减分的前提下，战队总成绩为AWD PLUS环节得分+靶场环节得分（归一化之后）加权之和。

二、AWD PLUS 环节

1. AWD PLUS为动态攻防兼备的比赛模式，综合考核参赛战队的漏洞发现、漏洞挖掘、漏洞修复、漏洞利用以及即时策略的能力。
2. 此模式得分分为攻击得分和防守得分，都采用同样全新动态计分方式。每个战队拥有相同的起始分数作为资产，及相同配置的靶机（GameBox）作为题目。每道题目都会提供一个附件包，供参赛者进行分析。每道题目的攻击模式和防守模式分别以一个轮次为计分单位，在同一个轮次内，攻击成功或防守成功都可以得分。每轮时间10分钟。
3. 攻击模式：参赛战队的任何队员都可以对任意一个或多个GameBox的预置漏洞进行利用，拿到flag值在平台提交成功，即认为该队员有能力对这一GameBox的漏洞进行利用，在题目关闭前的每一个攻击轮次内，成功完成这一GameBox漏洞利用的战队每个轮次都可在该题目中获得攻击分。

4. 防守模式：参赛战队的任何队员都可以对任意一个或多个 GameBox 中的预置漏洞，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，平台会在验证环境中执行修补包中的 update.sh 文件，并执行 check 程序和 exp 脚本。当 check 程序判断服务正常，且 exp 脚本利用失败时，判定该 GameBox 防守成功，在题目关闭前的每一个防守轮次内均可得到该题的防守分。
5. 动态积分：每道题目的攻击、防守各拥有初始分值（500分），每道题目的攻击、防守分值将根据得分队伍的数量进行动态调整，每增加1个攻击或防守成功的得分战队，该题目下一轮次的攻击或防守分值会随之下降，直至分别降到最低值（50分）。
6. 异常扣分：战队因上传防御包或其他原因导致题目服务不可用，判定此题状态为服务异常，如果在题目关闭前的每一个防守轮次结束之前仍然为服务异常的话，每一轮次都会扣除 $500 * 0.4$ 的积分。（注：防守失败不算异常，如果出现服务异常状态而又不能马上修补成功的话，可以上传一个普通包进行防守判定，使题目状态恢复到正常）
7. 重置次数：若某参赛队的 GameBox 服务出现异常导致无法进行攻击时，该队伍可点击重置按钮进行重置，注意每题重置赛题次数不同，具体请参见比赛界面。
8. 题目切换：比赛默认开放5道赛题，每道题目上线时都是绿灯状态，当平台判定题目答题价值不高时，题目或切换成红灯状态提

示1小时后将会下线。题目下线后切换新题上线，赛场上继续保持5道题目在线。在比赛结束倒数一小时内达到题目切换条件时不再进行题目切换。

9. 权重分配：半决赛AWD PLUS环节的权重为8000。总决赛AWD PLUS环节的权重为6500。

三、靶场环节

靶场演练环节中，针对关键信息基础设施行业进行了平行仿真的场景模拟，旨在考核参赛选手在模拟真实的场景中进行网络安全风险的发现和检测能力。参赛选手以战队为单位进入到靶场中完成既定目标。靶标场景的不同节点中，预置了多个flag。进入靶场的战队在靶场漫游时，设计渗透路径，获取更高权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。

总决赛阶段靶场演练模式面向所有战队全程开启。半决赛阶段靶场演练模式会按时开启，截止到开启前15分钟时，每组积分榜排名靠前的部分战队有资格进入靶场进行测试演练，答题端页面会提示靶场赛的开启和关闭时间。有资格进入靶场的战队AWD PLUS攻防环节不中断。

半决赛靶场环节的权重为2000。总决赛靶场环节的权重为3500。

半决赛靶场开启规则：

1. 12:45确定第一场靶场演练入围名单，由每个分组积分榜排名前12的队伍组成，合计48支，于13:00 - 15:00开放第一场靶场演练。
2. 15:45确定第二场靶场演练入围名单，去掉第一场入围者后，每个分组积分榜前12名可以进入，合计48支，于16:00 - 18:00开放第二场靶场演练。
3. 此环节中每个队伍进入独立靶场环境，不会互相干扰，靶标异常可以申请重置。
4. 此环节采用固定积分，场景内置多个flag，对应分值不等的固定分数，在开放时间内参赛者可以自由设计渗透路线。

四、扣分规则

1. 参赛选手禁止进行跨队交流、场外交流和连接互联网，一经发现赛后扣除参赛队总成绩的5%，再次发现终止比赛资格。
2. 比赛过程中禁止随意走动、大声喧哗，以及干扰他人比赛，经工作人员规劝拒不听从者，赛后扣除战队总成绩5%，再次发生则终止比赛资格。
3. 滥用“呼叫裁判”功能不正常表述问题，发布无意义或低俗、侮辱性内容者，在赛后扣除总分的2%。
4. 干扰比赛平台及设备，破坏赛场基础设施，影响比赛秩序，一经发现赛后扣除总分的10%。

五、其他规则

1. 裁判有权根据现场情况对违规、违纪战队进行减分、中止比赛、禁赛、通告等处理。
2. 裁判有权根据现场的积分情况，整体调整每队的初始分数值，以均衡AWD PLUS的得分收益。
3. 非预期解提交成功后得分有效。但题目价值降低时会被关灯下线，下线之后无法对该题作答或继续得分。
4. 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。
5. 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，否则不予回应。
禁止随意在场内走动。
6. 为维护现场秩序，避免跨战队交流，去洗手间请通过平台申请。经过工作人员确认后可以凭申请人参赛证从相应出口有秩序去洗手间。申请通过后半个小时没有抵达指定出口，则需要重新申请。

2020年第二届“网鼎杯”网络安全大赛组委会

2020年11月21日