赛宁网安

第四届“强网”拟态防御
国际精英挑战赛 参赛指南

南京赛宁信息技术有限公司

2021 年 10 月 4 日

1. 赛事简介

第四届“强网”拟态防御国际精英挑战赛计划于 2021 年 11 月 9 日至 11 月 12 日在南京江宁区网络通信与安全紫金山实验室举办，中国工程院、南京市人民政府、网络通信与安全紫金山实验室、中国网络空间安全协会主办，江宁区人民政府、南京江宁经济技术开发区管委会、中国网络空间内生安全技术与产业联盟承办，由南京赛宁信息技术有限公司提供赛事技术支撑。

因全球受新冠病毒影响，本届赛事将采用线上的方式举办，再次为全球顶尖战队提供机会，向邬江兴院士基于拟态防御理论的系列科研成果发起挑战，本届大赛通过加入同类型商用设备在安全性上的测试对比，与参赛队伍以及全球关注者深入探讨拟态防御原理以及理念，并通过对比测试向全球关注者展现拟态防御在主动防御领域的领先性以及有效性。

本届比赛首次引入商用设备和拟态构造设备对比测试的模式，参赛设备规模空前，包括 20 套典型商用网络设备和 30 套拟态构造网络设备，覆盖了路由、交换、Web 服务、域名服务、文件存储及云应用等互联网典型设备场景。

另一亮点是，本届比赛首次引入邬江兴院士团队自主研制的自动驾驶内生安全原理验证系统，在白盒积分争夺赛环节增加 16 款商用 ADAS 系统产品以及组建的拟态 ADAS 系统接入比赛,供参赛战队进行漏洞挖掘并按照规则计分。比赛进行同时，为增加比赛的挑战性和趣味性，本届大赛新增实车验证环节，实车验证时间安排在 2021 年 11 月 12 日 9:00-12:00。实车将搭载非拟态 ADAS 系统和拟态 ADAS 系统。主办方将根据评估，选择扰动环节中漏洞危害高和逃逸成功（需描述详细的漏洞发现及触发过程步骤、漏洞利用脚本或程序等）

且有意愿参与实车验证的参赛队伍，每支队伍有效验证时间为 1 小时，进行远程实车验证，对能够通过非拟态系统实际影响车辆的参赛队伍，额外奖励 5000 元，对能够利用拟态系统实际影响车辆的参赛队伍，额外奖励 10000 元。此部分仅为验证环节，不参与计分。

本届赛事采用线上模式并通过互联网全球同步直播赛况，展现了紫金山实验室对拟态防御安全性和稳定性的信心，必将成为全球网络安全竞赛的新标杆。

本届大赛参赛队伍采用特邀以及线上预选赛两种方式入围，特邀战队 18 支，线上资格赛入围战队 30 支。线上预选赛面向全球战队开放报名。

2. 组织机构

（一）主办单位：　中国工程院

南京市人民政府

网络通信与安全紫金山实验室

中国网络空间安全协会

（二）承办单位：　江宁区人民政府

南京江宁经济技术开发区管委会

中国网络空间内生安全技术与产业联盟

（三）支持单位：　南京赛宁信息技术有限公司

3. 赛制介绍

“强网”拟态防御国际精英挑战赛实际是“人-机对抗”的网络安全竞赛模式，颠覆了传统“人-人对抗”的CTF竞赛模式。本次“强网”国际拟态精英挑战赛通过提前进行的线上预选赛进行参赛队伍竞争入围，正式挑战赛延续并升级了独创的 “BWM”赛制（BWM3.0），其中B代表黑盒积分争夺赛（Black-Box Competition for points）、W代表白盒积分争夺赛（White-Box Competition for points）、M代表巅峰挑战赛（Mountain Challenge）。该赛制既挑战选手的技术水准，又考验选手的策略能力。

本届大赛具体赛制分布如下：

（1） 线上预选赛（Jeopardy）

（2） 黑盒积分争夺赛

黑盒积分争夺赛部分的黑盒测试对象设备包含拟态构造设备和商用设备。

a) 黑盒拟态推理赛

b) 黑盒安全测试赛

（3） 白盒积分争夺赛

a) 白盒资格赛（Jeopardy）

b) 拟态构造设备白盒注入安全测试

c) ADAS设备安全测试

d) ADAS系统漏洞实车验证（不参与计分）

（4） 巅峰挑战赛

拟态构造体系化网络场景安全测试

4. 竞赛日程

（1） 现场开赛仪式

2021 年 11 月 9 日 11:00-12:00（1 小时）

开幕式同时，主办方将通过 ZOOM 与各战队进行远程视频连线，并全球直播（11 月 8 日可能进行提前连线测试）。

（2） 黑盒积分争夺赛（全程开启）

2021 年 11 月 9 日 12:00-11 月 12 日 12:00（72 小时）

（3） 白盒积分争夺赛

a) 白盒资格赛

2021 年 11 月 9 日 12:00-11 月 12 日 12:00（72 小时）

b) 拟态构造设备白盒注入安全测试

2021 年 11 月 9 日 13:00-11 月 12 日 12:00（71 小时），整体赛程分为四个时间段，每小时一轮：

i. Day1：2021 年 11 月 9 日 13:00-24:00

ii. Day2：2021 年 11 月 10 日 9:00-24:00

iii. Day3：2021 年 11 月 11 日 9:00-24:00

iv. Day4：2021 年 11 月 12 日 9:00-12:00

c) ADAS 设备安全测试：

2021 年 11 月 9 日 13:00-11 月 12 日 12:00（71 小时），整体赛程分为四个时间段，每小时一轮：

i. Day1：2021 年 11 月 9 日 13:00-24:00

ii. Day2：2021 年 11 月 10 日 9:00-24:00

iii. Day3：2021 年 11 月 11 日 9:00-24:00

iv. Day4：2021 年 11 月 12 日 9:00-12:00

d) ADAS 系统漏洞实车验证：

2021 年 11 月 12 日 9:00-11 月 12 日 12:00（3 小时）

（4） 巅峰挑战赛：2021 年 11 月 9 日-11 月 12 日：当有一支队伍攻破所有的拟态构造黑盒设备后，面向所有的战队开启，截止到 2021 年 11 月 12 日 12:00（≤72 小时）

竞赛阶段	DAY 1 11.9				DAY 2 11.10				DAY 3 11.11				DAY 4 11.12			
	12:00	18:00	20:00	24:00	09:00	12:00	20:00	24:00	09:00	12:00	20:00	24:00	09:00	10:00	11:00	12:00
黑盒积分争夺赛																
白盒资格赛																
拟态构造设备 白盒注入安全测试	申请时间				休息				休息				休息			
ADAS 设备安全测试	申请时间				休息				休息				休息			
ADAS 系统漏洞 实车验证																
巅峰挑战赛					任一战队攻破所有的拟态黑盒设备后开启											

第四届“强网”拟态防御国际精英挑战赛时间安排

以上所有时间为东八区-中国北京时间。

5. 竞赛内容

本届竞赛设备种类更加丰富，设备数量创下新高，共计 50 台/套不同类型的网络设备参加竞赛，其中商用设备包括来自不同厂商的 7 类 20 台/套，拟态构造设备 7 类 30 台/套，包括黑盒测试设备 10 台/套，白盒测试设备 20 台/套，具体如表 1 和表 2 所示。ADAS 设备共 16 套。

表 1 商用设备类型数量

设备名称	商用路由器	商用 Web 防护设备	商用文件存储	商用域名服务器	商用数据库	商用交换机	商用云
设备厂商	3	3	3	2	3	3	3
设备数量	3	3	3	2	3	3	3
商用设备合计	20						

表 2 拟态构造设备类型数量

设备名称	拟态路由器	拟态 Web 服务器	拟态文件存储	拟态域名服务器	拟态数据库	拟态交换机 A	拟态交换机 B	拟态云-云平台	拟态云-某银行业务系统	拟态云-即时通信系统
黑盒数量	1	1	1	1	1	1	1	1	1	1
白盒数量	3	3	3	1	1	3	3	1	1	1
设备数量	4	4	4	2	2	4	4	2	2	2
拟态构造设备合 计	30									

5.1. 黑盒积分争夺赛

黑盒积分争夺赛的黑盒测试对象设备包括**商用设备（或商用设备保护的应用或网站）**和**拟态构造设备**，其中商用设备 7 种类型 20 套，拟态构造设备 7 种类型 10 套，共计 30 套。本次大赛首次引入商用设备作为挑战目标，和拟态防御构造设备同台竞技，通过同类设备的横向对比来检验被动防御和主动防御产品各自的安全性。

黑盒积分争夺赛全程开启，参赛战队可自行选择测试环境进行挑战，测试环境不体现是否为拟态构造设备或商用设备，需要由选手在黑盒测试过程中进行辨别。

黑盒设备的地址信息随附件发放，地址对应的名称在平台显示，平台不直接显示地址信息，请各参赛战队参见附件。

黑盒积分争夺赛分为两个阶段：**黑盒拟态推理**和**黑盒安全测试**。

在**黑盒拟态推理**阶段，参赛战队针对 30 套黑盒参赛设备运用技术手段分析并识别其中的 10 套黑盒拟态构造设备。得出结果后，参赛战队提交的分析报告给裁判组，如果识别正确，将获取一定的积分，如果识别错误，将扣除一定的积分，允许多次提交报告。**一个战队正确识别某一种拟态构造设备后，拟态构造设备将面向全场披露自身的详细信息，包括 CPU、操作系统、软件版本等等（各个拟态构造设备披露信息不同），该拟态构造设备的推理环节结束，六个小时之后未被识别出的拟态构造设备赛事方将主动披露设备形态。**

在**黑盒安全测试**阶段，参赛战队通过对设备进行漏洞的发现、挖掘与利用，尝试获取控制权限或者使得拟态防御设备裁决器发生异常报警，并提交漏洞

报告，裁判组依据漏洞报告审核挑战过程判定得分是否有效，并根据漏洞危害等级给予相应分数，每款设备被攻破三次后将自动下线。

本次黑盒积分争夺赛完善了计分方式，发现漏洞、利用漏洞等均可得分，详细计分方式见第 7.1 章节。

5.2. 白盒积分争夺赛

白盒积分争夺赛包含**白盒资格赛**和**拟态构造设备白盒注入安全测试**两个阶段。**白盒资格赛**的积分作为申请**拟态构造设备白盒挑战**的资格条件。需要满足一定积分额度才可以进行拟态构造设备白盒挑战申请，申请白盒挑战消耗白盒资格赛的积分。

5.2.1 白盒资格赛

白盒资格赛包含若干道漏洞挖掘和利用挑战题，参赛战队会根据解题顺序获得不同分数。

本次将由各拟态构造设备方进行主要命题工作，从而将拟态防御技术以及理念应用到网络安全赛事；

另外新增新型高安全网络协议破解方向的赛题（High Security VPN，HS-VPN）；

其余赛题考核方向包括 PWN 和 Web 等类型；

白盒资格赛积分用于申请拟态构造设备白盒注入安全测试。

5.2.2 拟态构造设备白盒注入安全测试

拟态构造设备白盒注入安全测试采取让步方式，开放拟态构造设备的某一

执行体，参赛队伍通过在该执行体中植入后门的情况下，以独占方式完成对拟态防御设备中指定目标的指定操作，尝试突破拟态机制，造成指定目标的指定逃逸状态。

拟态构造设备白盒注入安全测试按轮次进行，每小时 1 轮，参赛战队可以同时申请 **3 个不同类型**的白盒设备，申请需要冻结对应的白盒资格赛分数。挑战开始后将扣除冻结的分数，变更挑战目标或放弃排队不消耗分数。每个战队最多可挑战同一类型白盒设备 3 次。

拟态构造设备白盒注入安全测试详细流程说明见第 6 章。

5.2.3 ADAS 设备安全测试

本次大赛提供 16 款 ADAS 系统产品以及组建的拟态 ADAS 系统接入比赛进行漏洞挖掘，ADAS 系统漏洞挖掘比赛中包含漏洞挖掘计分以及扰动计分、逃逸计分方式，均采用分级计分方式，每级难度递增，积分也相应递增，本环节得分计入大赛总成绩。

ADAS 设备安全测试按轮次进行，每轮测试时间 50 分钟，参赛战队可根据平台资源池进行申请（ADAS 设备与当前轮次申请的白盒设备最多同时申请三款），申请需要冻结对应的白盒资格赛分数。挑战开始后将扣除冻结的分数，变更挑战目标或放弃排队不消耗分数。申请成功过后主办方将开放接入所申请 ADAS 设备跳板机的权限。

ADAS 设备安全测试详细流程说明见第七章。

5.2.4 ADAS 系统漏洞实车验证

为增加比赛的挑战性和趣味性，本届大赛新增实车验证环节，实车将搭载非拟态 ADAS 系统和拟态 ADAS 系统。主办方将根据评估，选择扰动环节中漏洞危害高和逃逸成功（需描述详细的漏洞发现及触发过程步骤、漏洞利用脚本或程序等）且有意愿参与实车验证的参赛队伍，每支队伍有效验证时间为 1 小时，进行远程实车验证，对能够通过非拟态系统实际影响车辆的参赛队伍，额外奖励 5000 元，对能够利用拟态系统实际影响车辆的参赛队伍，额外奖励 10000 元。此部分仅为验证环节，不参与计分。

5.3. 巅峰挑战赛

当有一支战队攻破所有拟态构造黑盒设备后，巅峰挑战赛场景开启，所有参赛战队可以向巅峰挑战赛场景发起黑盒挑战，突破拟态构造的体系化防御场景并成功篡改文件存储系统目标元数据，提交完整报告通过裁判组审核，确定挑战是否成功。

6. 竞赛流程

6.1. 黑盒积分争夺赛流程

黑盒积分争夺赛测试对象设备包括商用设备和拟态构造设备两种。比赛前八个小时是拟态推理阶段，需要选手主动去识别拟态构造设备，八个小时之后披露所有设备形态，直至所有设备被全部攻破为止，整个过程对全部战队开放挑战。参赛战队不需要使用积分申请，根据赛事方提供的设备入口信息即可对设备进行黑盒安全测试。

6.2. 白盒积分争夺赛流程

- **申请条件和积分消耗说明**

1) 初次申请：参赛战队白盒资格赛积分≥300 分时，参赛战队可以向任一设备（包含拟态构造设备以及 ADAS 设备）发起白盒挑战初次申请并冻结对应分数，单个类型设备挑战开始后将扣除 300 积分。
2) 同一类型的设备（包含拟态构造设备以及 ADAS 设备）二次申请：参赛战队白盒资格赛队积分≥400 分时，参赛战队可以向同一类型的拟态构造设备发起白盒挑战第二次申请并冻结对应分数，挑战开始后将消耗 400 积分。
3) 同一类型的设备（包含拟态构造设备以及 ADAS 设备）三次申请：参赛战队白盒资格赛队积分≥500 分时，参赛战队可以向同一类型的拟态构造设备发起白盒挑战第三次申请并冻结对应分数，挑战开始后将消耗 500 积分。
4) 参赛战队可以同时申请 3 个不同类型的设备（包含拟态构造设备以

及 ADAS 设备），系统冻结对应分数。开始挑战后，扣除对应分数。**参赛战队可能在下一轮次中挑战 2 个或 3 个类型的设备，参赛战队可以同时挑战，也可以提前放弃或者变更部分挑战目标。（进入准备挑战的状态下，不可更改）**

- **每轮时间说明**

平台时间：东八区-北京时间。

申请时间：X:00 - X:50。例如第一轮申请时间为 13:00 - 13:50，第二轮申请时间为 14:00 - 14:50。在申请时间内可以变更挑战目标和放弃挑战，变更挑战目标和申请新的挑战将按时间重新排队。

重置时间：X：50 - (X+1):00，如第一轮重置时间为 13:50 - 14:00，第二轮重置时间为 14:50 - 15:00。在重置时间内不允许申请、变更挑战、放弃挑战。（第 0 轮重置时间也不允许变更）

挑战时间：（X+1）：00 - （X+1）：50。

详细轮次请查看附件 2：《白盒积分争夺赛注入安全测试挑战申请和挑战轮次表》

- **拟态构造设备白盒注入安全测试挑战说明**

挑战开始后，参赛战队向拟态构造设备所提供的指定执行体进行后门注入，注入后门后点击“注入完成”按钮，注入时间最长不超过 30 分钟。注入完成或超时后，平台将含有后门的执行体重新部署到拟态构造设备中。比赛平台会自动进行策略切换，参赛战队可以向拟态构造设备发起攻击。

参赛战队对特定拟态构造白盒设备进行突破，攻击行为造成裁决器的判罚，平台将对该执行体进行清洗后上线。

对特定拟态构造设备突破的过程中，队伍攻击行为造成裁决器的告警达到10次，或整体时间达到50分钟（执行体注入+设备突破），则本轮该设备白盒正式赛结束。

- **ADAS设备安全测试挑战说明**

本届大赛新增ADAS系统漏洞挖掘的比赛环节（本环节开始于大赛的白盒积分争夺赛），提供16套市面上主流的ADAS系统产品，编号分别为01、02、03、04、05、06、07、08、……、16，各参赛队伍根据“先到先选”的原则，可在参赛平台上申请未被占用的编号ADAS系统进行漏洞挖掘，并在申请时需提供所选择的跳板机操作系统，选中后该ADAS系统的有效占用时间为50分钟，过时释放，若还需要漏洞挖掘，将重新排队参与下一次的漏洞挖掘。

挑战开始后，参赛战队通过开放的跳板机接入方式申请成功的ADAS系统，接入占用时长为50分钟，到达50分钟后，本轮接入测试结束。跳板机（共16个跳板机）接入大赛系统（大网），跳板机根据参赛队伍需求，可配置Linux和Windows操作系统（只能选择一个操作系统的跳板机），比赛开始后参赛队伍将需要的工具传输到跳板机中，即可开始对接入跳板机的ADAS系统进行漏洞挖掘。跳板机信息参考如下：

Windows跳板机：win10 企业版，4GB内存、4核，80GB磁盘空间，2个网卡，C、D两个盘符（参赛队伍工具文件请放置在D盘中），用户名/密码：test/123456，开放远程桌面。

Linux 跳板机：ubuntu 20.04、4GB 内存、4 核，80GB 磁盘空间，2 个网卡，用户名/密码：test/123456，开放 SSH、远程桌面。

!!! 注意：

- 比赛所用的 ADAS 系统均是市面上主流产品，任何参赛团队不得外泄 ADAS 系统的厂家信息和漏洞信息，否则将承担相关责任；
- 攻击团队漏洞挖掘时不得故意对 ADAS 系统进行不可恢复的攻击行为，否则将扣除大赛总积分的 10%，并提前结束当前 ADAS 设备测试；
- ADAS 系统开放接口：CAN 接口，网络接口或 USB 调试口。
- 除主办方个别提供的配套软件以外，不允许在跳板机上安装与设备配套的编程调试软件。

7. 竞赛计分规则

第四届“强网”拟态防御国际精英挑战赛包括多款拟态构造设备和商用设备。每个拟态构造设备触发裁决器异常和成功突破设备的标准不同，请参赛战队详细阅读和学习附件 3《拟态构造设备白盒注入安全测试得分判定标准》。

7.1. 黑盒积分争夺赛

7.1.1 黑盒拟态推理赛

参赛战队首先对黑盒测试设备靶标进行**拟态判别，判断是否是拟态构造设备，判断成功一次将获取 1000 分，判断错误一次将扣去 1000 分。同时拟态设备将面向全场披露自身的详细信息，包括 CPU、操作系统、软件版本等等（各个拟态设备披露信息不同），该拟态构造设备的推理环节结束。通过提交报告**

至裁判组，由裁判组人工评判，同一拟态构造设备不可重复得分。部分设备在推理环节结束后将直接下线，不参与后续环节，赛事平台中会给出提示信息。

7.1.2 黑盒安全测试赛

- **商用设备黑盒通用计分规则**

以参赛队伍通过挖掘利用设备漏洞造成异常输出为标准，每个设备作为目标根据选手攻击情况以及危害等级设定分值，参赛选手发现漏洞或利用成功后需通过平台提交漏洞报告至裁判组，漏洞报告应包含且不限于漏洞点、漏洞利用脚本、漏洞利用成效等相关说明以及截图证明，有必要可携带附件提交，由裁判组人工审核并根据报告成功复现后进行评判危害等级，裁判组人工审核通过后更新成绩。商用黑盒设备仅有提交漏洞报告得分一种手段，部分商用设备中预设有 flag 文件，请将 flag 文件以及 flag 值附带在报告中。

参赛战队可多次提交报告。

漏洞成功利用作为漏洞危害级别判定的前提条件。

漏洞危害级别以及给分标准如下(若部署应用和其他设备存在防护与被防护关系则依据组委会现场判定为准)：

级别	危害等级	分值	参考说明
Level 3	轻微影响	2000	1.普通信息泄漏，可获取设备基础信息但并不能造成实质危害。如明文存储的密码、web 路径遍历和系统路径遍历漏洞等。 2.其他危害较低的漏洞，包括但不限于反射型跨站

级别	危害等级	分值	参考说明
			脚本攻击漏洞（包括反射型 DOM-XSS）、普通跨站请求伪造（CSRF）、URL 跳转漏洞等。
Level 2	一般影响	3000	1.需交互才能获取管理身份信息的漏洞。包括但不限于存储型 XSS、反射型 XSS、DOM-XSS、重要敏感操作的 CSRF。 2. 普通越权操作，包括但不限于绕过限制修改用户资料、执行用户操作等。
Level 1	严重危害	5000	1. 直接获取系统权限的漏洞（服务器权限、PC 客户端权限），包括但不限于远程命令执行、任意代码执行、上传获取 Webshell、SQL 注入获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）等漏洞。 2. 敏感信息越权访问，包括但不限于绕过认证直接访问管理后台、重要后台弱密码、获取大量内网敏感信息的服务器端请求伪造（SSRF）漏洞等。 3. 攻击设备服务，使设备提供的服务不能正常运行（除 DOS 等拒绝服务攻击）。 4. 攻击设备部署的应用，使设备部署的应用遭到破坏。 5. 授权后的 get root shell，由基础权限获取到 root 权限，对设备有完整的控制权限。

- **拟态构造设备黑盒计分规则**

拟态构造设备黑盒安全测试采用分层分级的计分方式，共分为 4 级积分：查找漏洞、裁决器异常报警、设备瞬时逃逸和稳定逃逸，每级的难度递增，

积分也相应递增。其中查找漏洞根据不同的危害级别分为三种不同的计分层级，具体见下。

（1） 查找漏洞 计分规则

本届大赛拟态构造设备黑盒安全测试部分新增查找漏洞环节，如参赛战队发现疑似但无法利用的漏洞，可提交漏洞报告至裁判组，由裁判组人工评判给予相应分数，人工审核通过后更新成绩。

查找漏洞环节参赛战队可多次提交报告。

根据漏洞类型，计分标准如下：

级别	漏洞类型	分值	参考说明
Level 2	执行体漏洞	2000	发现拟态构造设备执行体中的漏洞
Level 1	拟态括号漏洞	5000	发现拟态构造设备拟态括号中的漏洞

（2） 裁决器异常报警 计分规则

单独拟态构造设备对执行体的漏洞挖掘利用：以参赛队伍通过挖掘利用执行体漏洞造成执行体输出触发裁决器异常报警为标准，每个拟态构造设备的每个执行体作为攻击目标设定动态分值，初始分值 10,000 分，动态计分公式为：$F(x)=1000+[(48-x)/47]^2*9000$。根据参赛队伍通过挖掘利用执行体漏洞造成裁决器针对指定目标有异常报警的队伍数量次序递减，人工审核通过后更新成绩。

（3） 瞬时逃逸 计分规则

单独拟态构造设备瞬时逃逸突破：队伍如突破裁决机制造成指定目标的逃

逸状态，但并不能稳定利用，控制拟态构造设备修改其中的指定目标数据。

参赛队伍必须及时提交完整攻破拟态构造设备的渗透报告至裁判组，由裁判组判定合规后，得分有效，每个拟态构造设备采用动态计分。初始分值为50,000 分，动态计分公式为：F（x）=10000+［（48-x）/47]² * 40000。根据突破队伍数量按次序递减。

（4） 完全逃逸 计分规则

单独拟态构造设备完全逃逸突破：队伍如完全突破裁决机制造成指定目标的完全逃逸状态，控制拟态构造设备修改其中的指定目标数据，可稳定利用且逃逸时长超过 5 分钟。

参赛队伍必须及时提交完整攻破拟态构造设备的渗透报告，由裁判组判定合规后，得分有效，每个拟态构造设备采用动态计分。初始分值为 100,000 分，动态计分公式为：F（x）=10000+［（48-x）/47]² * 90000。根据突破队伍数量按次序递减。

7.2. 白盒积分争夺赛

7.2.1 白盒资格赛

白盒积分抢夺赛采用国际常用的 CTF Jeopardy 模式，提供 10 道漏洞挖掘和利用挑战题题目。参赛队伍通过互联网进行题目挑战，挑战成功后获得该题目得分。

1、 使用严格防作弊机制，每个题目不同队伍 Flag 均不同；

2、 每个题目根据挑战队伍解题顺序进行分值递减，解题用时较短的队伍

获得的分值越高；

3、 每个题目根据难度设置不同的初始分值，同一个题目第 x 个解出队伍得分 F（x）=（Y/48）*（48-x+1），Y=初始分值

4、 参赛战队通过白盒资格赛获得分数，白盒积分争夺赛会消耗本环节得分。

7.2.2 拟态构造设备白盒注入安全测试

（1） 裁决器异常报警 计分规则

1) 单独拟态构造设备对执行体的扰动：参赛队伍通过执行体后门工具影响任一执行体的输出，造成任一执行体指定目标数据输出异常为标准，每个拟态构造设备的每个执行体作为攻击目标设定动态分值，初始分值 3,000 分，动态计分公式为：F（x）=300+ [（48-x）/47]² * 2700。根据突破队伍数量按次序递减。

2) 每个拟态构造设备有 3 个执行体，其中 1 个执行体已设置后门。攻击任一执行体触发裁决器第一次异常报警，经人工审核通过后获得当前执行体分值，之后拟态构造设备将清洗后重新上线，清洗过程中不允许攻击。

3) 攻击同一执行体触发裁决器第二次及更多次异常报警，经人工审核通过后会二次得分，第二次得分当前执行体分值的 1.5 倍。

（2） 瞬时逃逸 计分规则

单独拟态构造设备瞬时逃逸突破：队伍如突破裁决机制造成指定目标的逃逸状态，但并不能稳定利用，控制拟态构造设备修改其中的指定目标数据。

参赛队伍必须及时提交完整攻破拟态构造设备的渗透报告至裁判组，由裁判组判定合规后，得分有效，每个拟态构造设备采用动态计分。初始分值为10,000 分，动态计分公式为：F（x）=1000+［（48-x）/47］² *9000。根据突破队伍数量按次序递减。

（3） 完全逃逸 计分规则

单独拟态构造设备注入突破：队伍如通过执行体后门，完全突破裁决机制造成目标的完全逃逸状态，控制拟态构造设备修改其中的指定目标数据，可稳定利用且逃逸时长超过 5 分钟。

参赛队伍必须及时提交完整攻破拟态构造设备的渗透报告，由裁判组判定合规后，得分有效，每个拟态构造设备采用动态计分，初始分值为 20,000 分，动态计分公式为：F（x）=2000+［（48-x）/47］² * 18000。根据突破队伍数量按次序递减。人工审核通过后更新成绩。

7.2.3 ADAS 设备安全测试

ADAS 系统的评分标准分为漏洞报告、利用漏洞造成扰动以及拟态逃逸三类评分标准，其中漏洞报告和利用漏洞报告造成扰动两类不重复进行计分，按照最高得分进行计分，拟态逃逸单独计分。所有参赛队伍得分将以漏洞报告为准，未提交漏洞报告或漏洞报告验证无效不得分。

- 漏洞报告计分标准

参赛队伍挖掘出了 ADAS 漏洞，并需提交挖掘到的漏洞报告（需描述详细的漏洞发现及触发过程步骤），但并未利用漏洞造成 ADAS 系统输出扰动。

根据漏洞的严重程度，主要分为三级，计分标准如下：

级别	漏洞类型	分值
Level3	信息泄露、弱口令，基于原生系统命令导致设备工作异常等漏洞	1000
Level2	基于设备代码健壮性缺陷导致的 DOS 等漏洞	2000
Level1	基于设备代码安全隐患导致的代码执行、远程读写等漏洞	3000

如参赛战队发现疑似但无法利用的漏洞，可提交漏洞报告至裁判组，由裁判组人工评判给予相应分数，人工审核通过后更新成绩。

参赛队伍本轮漏洞挖掘获得的得分，综合计算后计入大赛总积分，参与大赛的奖励评比。

- 漏洞扰动计分标准

在 ADAS 标准输出下，参赛队伍通过挖掘利用 ADAS 系统漏洞成功屏蔽或篡改该 ADAS 的感知决策报文则认定为扰动得分，其他扰动不得分，并提交详细的漏洞利用过程报告。

根据漏洞扰动的严重程度，主要分为三级，计分标准如下：

级别	漏洞类型	分值
Level3	信息泄露、弱口令，基于原生系统命令导致设备工作异常等漏洞造成的扰动	2000
Level2	基于设备代码健壮性缺陷导致的 DOS 等漏洞造成的扰动	3000

级别	漏洞类型	分值
Level1	基于设备代码安全隐患导致的代码执行、远程读写等漏洞造成的扰动	4000

- 拟态逃逸计分标准

计分标准：在 ADAS 标准输出下，屏蔽或篡改拟态 ADAS 系统输出的感知决策报文，并实现裁决逃逸，使该输出报文能够生效，需提供详细的漏洞利用报告。

瞬时逃逸突破：参赛队伍如突破裁决机制造成指定目标的逃逸状态，但并不能稳定利用，控制拟态构造设备修改其中的指定目标数据。

完全逃逸突破：队伍如完全突破裁决机制造成指定目标的完全逃逸状态，控制拟态构造设备修改其中的指定目标数据，可稳定利用且逃逸时长超过 5 分钟。

瞬时逃逸情况下，各参与攻击拟态 ADAS 的参赛队伍将平分 10000 分。

完全逃逸情况下，各参与攻击拟态 ADAS 的参赛队伍将平分 20000 分。

注意事项：（1）扰动/逃逸得分必须成功在其中一个/全部在线执行体输出报文中修改为指定给本战队 ADAS 自身的报文。凡是没有实现上面目标的扰动属于无效扰动，不会得分。输出报文修改为指定给其他战队的 ADAS 报文不得分。（2）必须通过攻击拟态设备自身并造成扰动或逃逸才可以得分，通过中间人劫持等只导致回显结果改变的攻击为无效攻击。

7.2.4 ADAS 系统漏洞实车验证

不参与计分。

7.3. 巅峰挑战赛

当有一支战队攻破所有拟态构造黑盒设备后，第四届赛事巅峰挑战赛场景面向所有战队开启。队伍突破拟态构造设备构建的体系化网络场景并成功修改其中指定目标数据，必须及时提交完整攻破巅峰挑战赛场景的解题报告，由裁判组判定合规后，得分有效。巅峰挑战赛的初始分值为 500,000 分，动态计分公式为：$F(x)=50000+[(48-x)/47]^2 * 450000$。根据突破队伍数量按次序递减，人工审核通过后更新成绩。

8. 总分和排名

队伍比赛总分为黑盒积分争夺赛、白盒积分争夺赛、巅峰挑战赛的总和，最终比赛排名将根据比赛总分进行名次排序，参赛队伍总分相同时，以得到当前分值时间靠前的队伍排名靠前。

9. 注意事项

1. 各参赛选手安装 Chrome 浏览器访问竞赛平台，不允许把自己账号泄露给其他人。

2. 每支参赛战队会分配 4 个 SSL VPN 账号，每个账号同时只能一个人登陆使用；

3. 参赛选手通过 SSL VPN 访问本次竞赛平台和竞赛环境，IP 地址为 VPN 自动分配，不允许人工修改；

4. 禁止不同参赛队伍合作，或者共享解题思路等任何比赛相关信息；

5. 参赛战队在单独拟态构造设备完全突破或逃逸、巅峰挑战赛场景突破，需通过压缩包方式上传 POC 或 Exploit 文档，以供裁判组审核；

6. 组织方有权要求参赛队伍在线立即提供任意攻击得分的 WP，如未能在给定时间内完成提交，则组织方有权判定参赛队伍的攻击得分无效，扣除相关得分和奖励；

7. 禁止攻击赛事平台，如果发现平台漏洞，请务必向运维团队报告，攻击赛事平台者一经发现立即取消所在战队参赛资格；

8. 禁止对参赛设备进行致瘫攻击，如发现致瘫攻击，立即取消所在战队

参赛资格；

9. 部分参赛所必须信息将通过邮件附件的形式发放，包含 VPN 信息、平台信息、赛题必要信息等，请各战队注意查收，并结合平台给予的信息进行比赛；

10. 关于比赛规则的调整和最终解释权归大赛组委会所有。

10. 奖项设置

第四届“强网”拟态防御国际精英挑战赛总奖金200万元，其中基础奖100万元，特别奖100万元。具体分配方案如下：基础奖按排名分配，设一、二、三等奖和优胜奖。参赛队伍总分≥100分，可以根据竞赛名次获得以下奖金：

一等奖42万元:第1名20万元；第2名14万元；第3名8万元；

二等奖20万元:第4-8名每队4万元；

三等奖24万元:第9-20名每队2万元；

优胜奖14万元:第21-48名每队5千元。

特别奖100万元：由突破拟态巅峰挑战赛场景的队伍平分。

附件 1、拟态设备简介

网络空间拟态防御（Cyber Mimic Defense，CMD）是国内研究团队首创的理论，为应对网络空间中不同领域相关应用层次上基于未知漏洞、后门、病毒或木马等未知威胁，提供具有普适创新意义的防御理论和方法。2016 年 11 月 17 日,攻坚团队的主要负责人邬江兴院士在第三届世界互联网大会上发布了该研究成果。

受生物界基于拟态现象的伪装防御启迪,CMD 理论在可靠性领域非相似余度架构基础上导入多维动态重构机制，造成视在功能不变条件下，目标对象内部的非相似余度构造元素始终在作数量或类型、时间或空间维度上的策略性变化或变换，用不确定防御原理来对抗网络空间的确定或不确定威胁。

相比于其他安全技术,CMD 既能为信息网络基础设施或重要信息服务系统提供不依赖于传统安全手段（如防火墙，入侵检测，杀毒软件等）的一种构造化内生安全增益或效应，也能以固有的集约化属性提供弹性的或可重建的服务能力，或融合成熟的防御技术获得超非线性的防御效果。

成套的拟态防御设备包括拟态路由器、拟态域名服务器、拟态 Web 服务器、拟态文件存储系统、基于拟态构造的 SaaS 云、拟态数据中心等。

1、拟态路由器

拟态路由器在其架构中引入多个异构冗余的路由执行体，同时引入了路由裁决、输入代理、调度清洗等拟态组件，实现多个路由执行体的“并行运行、单一呈现”。通过对路由器架构的拟态化构造，在保证功能性能不变的情况下，使拟态路由器能够不依赖于攻击特征实现对路由表篡改攻击的发现和

阻断，有效提升路由器安全性。

2、拟态域名服务器

拟态域名服务器以遏制域名解析服务漏洞后门的可利用性、建立内生安全防御机制、大幅提高攻击者的攻击难度和代价为出发点，可以在不改变现有域名协议和地址解析设施的基础上，通过拟态防御设备的增量部署，能够有效防御针对域名系统漏洞后门的域名投毒、域名劫持攻击等各种已知和未知攻击，能够提供安全可靠的域名解析服务。

3、拟态 Web 服务器

拟态 Web 服务器针对 Web 服务面临的安全威胁，根据拟态防御原理，在 Web 服务器的硬件平台层、操作系统层、虚拟化软件层、服务器软件层以及 Web 应用层设计功能等价、多样化的异构冗余执行体，通过拟态表决机制，阻断攻击链，并利用负反馈调度机制对执行体进行清洗恢复，极大地增加了 Web 服务运行环境中漏洞及后门的利用难度，在不影响 Web 服务功能、性能的前提下，保证 Web 服务的安全可信。

4、拟态文件存储系统

拟态文件存储系统面向大数据分布式存储系统所面临的威胁而设计，针对系统中需要核心防护的元数据功能和信息进行动态化、异构冗余化的保护。系统基于多样化的软硬执行环境搭建多个等价的元数据执行体，通过分发-裁决机制和动态调度策略屏蔽由漏洞和后门发起的攻击交互，配合清洗机制阻断攻击链，扰乱攻击者的探测和渗透过程。基于拟态化的元数据结构能够使分布式存储系统的核心数据和功能逻辑得到有效的安全防护，从而显著提升

整个系统提供文件存储服务的安全性。

5、基于拟态构造的 SaaS 云

基于拟态构造的 SaaS 云是针对云环境 SaaS 应用服务实例面临的漏洞和后门问题，在基础软硬件环境、云应用软件等层面引入异构化，构建运行环境及服务异构的冗余执行体，通过拟态裁决机制快速发现可疑执行体，并配合负反馈控制机制自动化完成下线、清洗、轮换等处置操作，在不影响 SaaS 应用服务功能、性能的条件下，极大地增加对 SaaS 应用服务的漏洞及后门的利用难度，确保提供安全可靠的云服务。

6、拟态数据中心

拟态数据中心管理平台面向通用数据中心所面临的威胁而设计，针对数据中心中需要核心防护的管理功能和信息进行动态化、异构冗余化的保护。本系统基于多样化的软硬执行环境搭建多个等价的数据中心管理系统执行体，通过分发-裁决机制和动态调度策略屏蔽由漏洞和后门发起的攻击交互，配合清洗机制阻断攻击链，扰乱攻击者的探测和渗透过程。基于拟态化的数据中心管理平台能够使数据中心中的管理业务得到有效的安全防护，从而显著提升整个数据中心的安全性。

7、拟态软件（运行时环境）

拟态软件（运行时环境）针对二进制程序面临的安全威胁，根据拟态防御原理，使程序自动以异构冗余的方式执行，通过拟态表决及拟态伪装机制，阻断攻击链，极大地增加了二进制程序中漏洞及后门的利用难度。

附件 2：《白盒积分争夺赛申请和挑战轮次表》

开放时段	申请轮次	申请时间	挑战轮次	挑战时间
2021 年 11 月 9 日 12:00-23:50	第 1 轮	12:00-12:50	第 1 轮	13:00-13:50
	第 2 轮	13:00-13:50	第 2 轮	14:00-14:50
	第 3 轮	14:00-14:50	第 3 轮	15:00-15:50
	第 4 轮	15:00-15:50	第 4 轮	16:00-16:50
	第 5 轮	16:00-16:50	第 5 轮	17:00-17:50
	第 6 轮	17:00-17:50	第 6 轮	18:00-18:50
	第 7 轮	18:00-18:50	第 7 轮	19:00-19:50
	第 8 轮	19:00-19:50	第 8 轮	20:00-20:50
	第 9 轮	20:00-20:50	第 9 轮	21:00-21:50
	第 10 轮	21:00-21:50	第 10 轮	22:00-22:50
	第 11 轮	22:00-22:50	第 11 轮	23:00-23:50
	第 12 轮	23:00-23:50	/	/
2021 年 11 月 10 日 9:00-23:50		/	第 12 轮	9:00-9:50
	第 13 轮	9:00-9:50	第 13 轮	10:00-10:50
	第 14 轮	10:00-10:50	第 14 轮	11:00-11:50
	第 15 轮	11:00-11:50	第 15 轮	12:00-12:50
	第 16 轮	12:00-12:50	第 16 轮	13:00-13:50
	第 17 轮	13:00-13:50	第 17 轮	14:00-14:50

开放时段	申请轮次	申请时间	挑战轮次	挑战时间
	第 18 轮	14:00-14:50	第 18 轮	15:00-15:50
	第 19 轮	15:00-15:50	第 19 轮	16:00-16:50
	第 20 轮	16:00-16:50	第 20 轮	17:00-17:50
	第 21 轮	17:00-17:50	第 21 轮	18:00-18:50
	第 22 轮	18:00-18:50	第 22 轮	19:00-19:50
	第 23 轮	19:00-19:50	第 23 轮	20:00-20:50
	第 24 轮	20:00-20:50	第 24 轮	21:00-21:50
	第 25 轮	21:00-21:50	第 25 轮	22:00-22:50
	第 26 轮	22:00-22:50	第 26 轮	23:00-23:50
	第 27 轮	23:00-23:50	/	/
2021 年 11 月 11 日 9:00-23:50		/	第 27 轮	9:00-9:50
	第 28 轮	9:00-9:50	第 28 轮	10:00-10:50
	第 29 轮	10:00-10:50	第 29 轮	11:00-11:50
	第 30 轮	11:00-11:50	第 30 轮	12:00-12:50
	第 31 轮	12:00-12:50	第 31 轮	13:00-13:50
	第 32 轮	13:00-13:50	第 32 轮	14:00-14:50
	第 33 轮	14:00-14:50	第 33 轮	15:00-15:50
	第 34 轮	15:00-15:50	第 34 轮	16:00-16:50
	第 35 轮	16:00-16:50	第 35 轮	17:00-17:50

开放时段	申请轮次	申请时间	挑战轮次	挑战时间
	第 36 轮	17:00-17:50	第 36 轮	18:00-18:50
	第 37 轮	18:00-18:50	第 37 轮	19:00-19:50
	第 38 轮	19:00-19:50	第 38 轮	20:00-20:50
	第 39 轮	20:00-20:50	第 39 轮	21:00-21:50
	第 40 轮	21:00-21:50	第 40 轮	22:00-22:50
	第 41 轮	22:00-22:50	第 41 轮	23:00-23:50
	第 42 轮	23:00-23:50	/	/
2021 年 11 月 12 日 9:00-11:50		/	第 42 轮	9:00-9:50
	第 43 轮	9:00-9:50	第 43 轮	10:00-10:50
	第 44 轮	10:00-10:50	第 44 轮	11:00-11:50

附件 3：《黑盒安全测试赛及白盒积分争夺赛得分判定标准》

1 黑盒安全测试赛

1.1 商用设备

1.1.1 商用路由器

参赛战队利用漏洞远程登录设备获取 flag，并提交 writeup 和 flag，flag 附加在报告中即可；

flag 格式固定为 flag{xxxxx}

1.1.2 商用 Web 防护设备

挖掘漏洞，并利用漏洞突破 3 套商用设备并进行篡改主页 index.html，主页篡改成功标准为：战队在 index.html 页面上添加 team+战队编号(比如战队编号为 01 的战队需在 index.html 页面上添加“team01”，即被认为篡改成功)，并提交漏洞报告，裁判组依据漏洞报告审核挑战过程判定得分是否有效，并根据漏洞危害等级给予相应分数，每款设备被攻破三次后将自动下线。

1.1.3 商用文件存储

1.1.3.1 商用文件存储 - 1

在给参赛队配发的资源中包含访问存储设备所需的账号及设备地址，各参赛队可通过 windows/linux 挂载访问设备，系统为各队分配了文件目录，同时也对写入权限和配额进行了限定。

攻击目标：对于第 x 号参赛队，篡改系统中指定目录/team_x/的权限控制机制，越权创建文件“team x_FlagInsertion”，写入战队信息内容。

得分判定： 成功在指定目录中创建文件及写入内容，即可得分。

注意事项：

(1)得分必须成功在指定目录中创建指定名称的文件并写入相应内容。凡是没有实现该目标的攻击属于无效攻击，不会得分。

(2)必须通过攻击存储设备自身并成功写入指定文件可以得分，通过中间人劫持等只导致客户端回显结果改变的攻击为无效攻击。

(3)参赛战队不允许进行 DDOS 攻击、破坏设备环境、篡改非自己队伍目标目录等影响其他选手正常比赛的攻击，如被第一次发现，不仅不得分数而且会另外扣除该队 1000 分，并提前结束本轮测试；如被第二次发现，则取消该队对商用文件存储的比赛资格。

1.1.3.2 商用文件存储 - 2&3

在给参赛队配发的资源中包含访问存储设备所需 client，系统为各队分配了文件目录，同时也对写入权限和配额进行了限定，这部分内容是由系统的元数据节点（即设备 IP 地址）进行管理维护的。

题目 1：越权写入

攻击目标：对于第 x 号参赛队，篡改系统中指定目录/team_x/的权限控制机制，越权创建文件“team x_FlagInsertion”，写入战队信息内容。

得分判定： 成功在指定目录中创建文件及写入内容，即可得分。

题目 2：获取 Flag

攻击目标：对于第 x 号参赛队，越权进入元数据节点，获取其/Flag 目录下本队伍编号对应的 Flag 文件。

得分判定： 成功获得 Flag 文件，内容正确，提交的 writeup 文件判定通过即可得分。

注意事项：

(1)得分必须成功在指定目录中创建指定名称的文件并写入相应内容。凡是没有实现该目标的攻击属于无效攻击，不会得分。

(2)必须通过攻击存储设备自身并成功写入指定文件可以得分，通过中间人劫持等只导致客户端回显结果改变的攻击为无效攻击。

(3)参赛战队不允许进行 DDOS 攻击、破坏设备环境、篡改非自己队伍目标目录等影响其他选手正常比赛的攻击，如被第一次发现，不仅不得分数而且会另外扣除该队 1000 分，并提前结束本轮测试；如被第二次发现，则取消该队比赛资格。

1.1.4 商用域名服务器

攻击信息：(1) 成功修改商用域名服务器指定域名的 www.dnstest.com.cn 解析结果至一个指定 IP 地址 3.4.5.6。

(2) 造成 DNS 服务软件崩溃。请使用构造 DNS 解析报文，使 DNS 服务器停止解析或程序 crash。

得分判定：(1) 成功修改指定域名的解析结果，触发 flag 上报结果即可得分。

(2)成功将域名服务宕掉，上报结果即可得分。

注意事项：(1) 通过中间人劫持等只导致客户端回显结果改变的攻击为无效攻击。(2) 参赛战队不允许进行 DDOS 攻击、虚拟机穿透宿主机等影响其他选手正常比赛的攻击，如被第一次发现，不仅不得分数而且会另外扣除该队 1000 分，并提前结束本轮测试；如被第二次发现，则取消该队比赛资格。

1.1.5 商用数据库

1.1.5.1 商用数据库 A

访问方式：

使用附件中提供的示例代码和驱动 JAR 包来连接和访问数据库。

示例代码 Main.java 文件中已经给出了数据库连接的 IP、端口、库名、用户名、密码。攻击者可自行修改示例代码完成攻击目标。

文件夹 数据库驱动 中的 JAR 包是数据库访问的 JDBC 驱动；

db*-1.0-SNAPSHOT.jar 是三种数据库访问的可执行 JAR 包，例如 java -jar dbA-1.0-SNAPSHOT.jar 命令可以完成数据库的连接和查询操作。

攻击目标：在示例代码指定的库名下创建 teamxxx 名称的数据表。

说明: teamxxx 中的 xxx 表示战队 ID。

1.1.5.2 商用数据库 B

访问方式：

使用附件中提供的示例代码和驱动 JAR 包来连接和访问数据库。

示例代码 Main.java 文件中已经给出了数据库连接的 IP、端口、库名、用户名、密码。攻击者可自行修改示例代码完成攻击目标。

文件夹 数据库驱动 中的 JAR 包是数据库访问的 JDBC 驱动；

db*-1.0-SNAPSHOT.jar 是三种数据库访问的可执行 JAR 包，例如 java -jar dbA-1.0-SNAPSHOT.jar 命令可以完成数据库的连接和查询操作。

攻击目标：在示例代码指定的库名下创建 teamxxx 名称的数据表。

说明: teamxxx 中的 xxx 表示战队 ID。

1.1.5.3 商用数据库 C

访问方式：

使用附件中提供的示例代码和驱动 JAR 包来连接和访问数据库。

示例代码 Main.java 文件中已经给出了数据库连接的 IP、端口、库名、用户名、密码。攻击者可自行修改示例代码完成攻击目标。

文件夹 数据库驱动 中的 JAR 包是数据库访问的 JDBC 驱动；

db*-1.0-SNAPSHOT.jar 是三种数据库访问的可执行 JAR 包，例如 java -jar dbA-1.0-SNAPSHOT.jar 命令可以完成数据库的连接和查询操作。

攻击目标：在示例代码指定的库名下创建 teamxxx 名称的数据表。

说明: teamxxx 中的 xxx 表示战队 ID。

1.1.6 商用交换机

1.1.6.1 商用设备 1

要求：免密登陆漏洞：选手免密登陆，获取设备 hostname：

1.1.6.2 商用设备 2

要求：远程命令执行漏洞：选手获取/etc/banner 文件内容

1.1.6.3 商用设备 3

要求：交换机 http 拒绝服务漏洞：选手自己提交验证报告

1.1.7 商用云

访问方式：

攻击者使用浏览器访问拟态云平台，用户名 testA，密码 testA_123

通过界面可以看到该用户属于项目 testProjectA。

目前系统已经预置了两个项目：testProjectA 和 testProjectB。

攻击目标：创建 teamxxx 命名的用户，且该用户属于项目 testProjectB。

说明: teamxxx 中的 xxx 为分配给战队的 teamid。

1.2 拟态设备

1.2.1 拟态路由器

黑盒挑战开始后，参赛战队的攻击目标是在设备上增加路由表项，得分方式为：在执行体上增加一条分配给本战队的路由表项，可以获得扰动得分；如果同时在过半数的执行体上增加一条分配给本战队的路由表项，使该表项能够通过路由裁决，就能获得逃逸得分。

路由信息如下所示，其中 xx 为战队编号:

目的 IP:　123.123.xx.0/24　下一跳：192.168.4.100

1.2.2 拟态 Web 服务器

挖掘漏洞，并利用漏洞成功篡改其中一个或多个执行体的主页 index.html，主页篡改成功标准为：战队在 index.html 页面上添加 team+战队编号（比如战队编号为 01 的战队需在 index.html 页面上添加“team01”，即被认为篡改成功)。共计以下 4 种情况能够得分：

1、找到漏洞

2、成功篡改执行体主页触发裁决器异常：参赛战队成功篡改某个执行体主页，导致裁决器判定不一致，并形成异常告警。

3、成功篡改执行体主页导致瞬时逃逸：参赛战队成功篡改多个执行体主页，且篡改后主页一致，访问拟态设备主页 index.html 的结果为该参赛战队篡改后结果，即认定拟态设备处于逃逸状态。逃逸状态不能稳定利用，即认定为瞬时逃逸。

4、成功篡改执行体主页导致完全逃逸：参赛战队成功篡改多个执行体主页，且篡改后主页一致，

访问拟态设备主页 index.html 的结果为该参赛战队篡改后结果，即认定拟态设备处于逃逸状态。逃逸状态能够稳定利用且持续时长超过 5 分钟，即可认定为完全逃逸。

各参赛战队不得删除其他战队添加的指定内容。裁判组会对攻击源和提交的报告进行判定得分。

1.2.3 拟态文件存储

在给参赛队配发的资源中包含访问存储所必需的 client 及各队对应的 cfg 文件，系统为各队分配了文件目录，同时也对访问权限和写入配额进行了限定，这部分内容是由系统的元数据节点（即设备 IP 地址）进行管理维护的。

攻击目标：对于第 *x* 号参赛队，篡改系统中指定的元数据目录/team_*x*/，越权创建文件“MMS_No*x*_FlagInsertion”，突破配额限制写入战队信息内容。

得分判定：（1）成功在一个在线执行体中达成攻击目标，并通过该目标触发裁决器异常报警，即可扰动得分；

（2）基于攻击目标，使得文件系统的篡改状态能通过外部访问稳定呈现**（持续 3 分钟）**，即可逃逸得分。

注意事项:

(1)扰动/逃逸得分必须成功在其中一个/全部在线执行体中创建指定名称的文件并写入相应内容。凡是没有实现上面目标的扰动属于无效扰动，不会得分。

(2)必须通过攻击拟态设备自身并造成扰动或逃逸才可以得分，通过中间人劫持等只导致客户端回显结果改变的攻击为无效攻击。

(3)参赛战队不允许进行 DDOS 攻击、破坏设备环境等影响其他选手正常比赛的攻击，如被第一次发现，不仅不得分数而且会另外扣除该队 1000 分，并提前结束本轮测试；如被第二次发现，则取消该

队对拟态文件存储的比赛资格。

1.2.4 拟态域名服务器

攻击目标：成功修改拟态域名服务器在线执行体对指定域名的解析结果至一个指定 IP 地址。

得分判定：(1) 成功修改其中一个在线执行体对指定域名的解析结果至一个指定 IP 地址，并触发裁决器异常报警，即可扰动得分；

(2) 同时修改全部在线执行体对指定域名的解析结果至一个指定 IP 地址，并使该映射关系持续（连续 5 分钟）通过裁决，即可逃逸得分。

注意事项：(1)扰动/逃逸得分必须成功修改其中一个/全部在线执行体的指定域名的解析结果至一个指定 IP 地址。凡是没有实现上面目标的扰动属于无效扰动，不会得分。 (2)必须通过攻击拟态设备自身并造成扰动或逃逸才可以得分，通过中间人劫持等只导致客户端回显结果改变的攻击为无效攻击。(3)参赛战队不允许进行 DDOS 攻击、虚拟机穿透宿主机等影响其他选手正常比赛的攻击，如被第一次发现，不仅不得分数而且会另外扣除该队 1000 分，并提前结束本轮测试；如被第二次发现，则取消该队对拟态域名服务器的比赛资格。

1.2.5 拟态数据库

访问方式：使用附件中提供的驱动程序（示例代码）来连接和访问数据库。攻击者可自行修改示例代码。

攻击目标：创建 teamxxx 命名的账号，并使用 teamxxx 账号创建 teamxxx 名称的数据表。xxx 为分配给战队的 teamid

得分判定：(1)基于攻击目标，触发裁决器异常报警，即可扰动得分；(2)基于攻击目标，查询到指定记录，即可逃逸得分。

注意事项：(1) 扰动得分必须基于攻击目标实现有效的裁决器异常报警，凡是没有基于攻击目标的异常报警，不会得分(2)必须通过攻击拟态设备造成扰动或逃逸才可以得分，通过中间人方式劫持服务显示结果的方式判为无效攻击。

1.2.6 拟态交换机 A

成功配置一条 ACL 规则。

战队编号 X∈（1-48），X 为分配给战队的 teamid

1) 创建 ACL：acl number 200X

2) 设置规则：rule 1 permit 192.168.20.X/0.0.0.0

3) 绑定到端口：traffic limit ingress acl number 200X 1 cir 1000

1.2.7 拟态交换机 B

攻击目标：利用交换机内部漏洞后门窃取交换机内配置文件。

得分判定：

1) 选手使用 tftp 方式将交换机配置文件传输到选手电脑，认定为突破设备得分；

2) 成功突破一个执行体，并开始文件传输，触发裁决器发出对 tftp 的异常报警，认定为扰动得分。

注意事项：

触发与赛题无关的其他扰动（非 TFTP、FTP 扰动）选手不得分。

1.2.8 拟态云-云平台

访问方式：攻击者使用浏览器访问拟态云平台,完成漏洞挖掘和注入攻击。

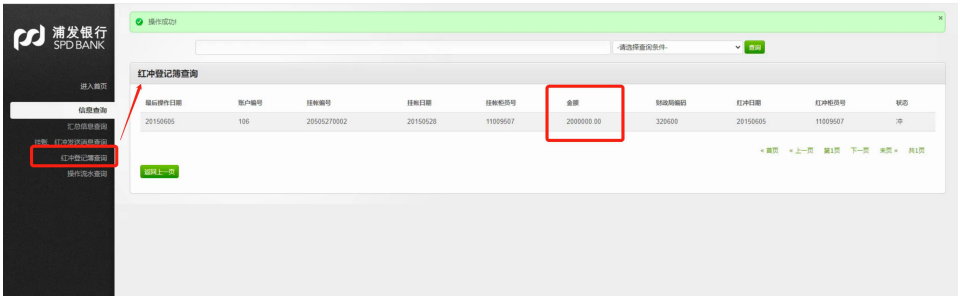
攻击目标：创建 teamxxx 命名的虚拟机，xxx 为分配给战队的 teamid

得分判定：（1）扰动得分：基于攻击目标，战队将原信息修改为其它值，并触发裁决器异常报警即可得分，其它扰动报警视为无效。（2）逃逸得分：基于攻击目标，战队篡改的信息能够通过外部访问，且使篡改后的数据信息持续（连续 5 分钟）通过裁决。

注意事项：（1）有效得分：只有通过达成上述攻击目标，并在外部访问触发扰动或逃逸才能得分。（2）无效攻击：篡改页面其它信息造成扰动或逃逸，不得分；通过中间人攻击劫持云应用的服务，并未对防护对象“真正”实施篡改，导致在外部呈现已篡改信息，视为无效行为，不得分；仅篡改执行体内的网页信息，而未对后台数据进行修改，造成扰动不得分。（3）罚分规则：通过关闭/重启云应用服务触发裁决扰动被视为违规，扣除 1000 分，并中止本轮挑战测试。

1.2.9 拟态云-某银行业务系统

攻击目标：银行缴费系统应用预置 1 条“红冲登记”记录信息（金额为 2000000.00，url 为：http://a.b.c.d:e/NTczfs /query/queryGzdjb.action?pageResultSet.pageInfo.currentPage=1），篡改该信息页的登记金额为指定的数值。例如，战队 01 篡改为 2010000.00，战队 48 篡改为 2480000.00。白盒执行体内预先植入了一个 shell，并有两个可用参数，分别为 f 和 t，可以利用这两个参数上传文件。



得分判定：（1）扰动得分：基于攻击目标，战队将金额修改为指定的数值，并触发裁决器异常报警即可得分，其它扰动报警视为无效。（2）逃逸得分：基于攻击目标，战队篡改的记录能够通过外部访问，且使篡改后的数据信息持续（连续 3 分钟）通过裁决。

注意事项：（1）有效得分：只有通过达成上述攻击目标，并在外部访问触发扰动或逃逸才能得分。

（2）无效攻击：篡改页面其它信息造成扰动或逃逸，不得分；通过中间人攻击劫持银行缴费应用服务，并未对防护对象“真正”实施篡改，导致在外部呈现已篡改信息，视为无效行为，不得分；仅篡改执行体内的网页信息，而未对后台数据库进行修改，造成扰动不得分。（3）罚分规则：通过关闭/重启银行缴费应用触发裁决扰动被视为违规，扣分并中止本轮挑战测试。

1.2.10 拟态云-即时通信系统

本赛题的解题目标为参赛者将战队名称添加到后勤部门组织架构中（篡改本地浏览器 Web 界面的方式无效），触发裁决器异常报警即可得分，其它扰动报警不得分。其中，突破设备逃逸的标准是同时在所有执行体用户 Web 界面后勤部门中添加战队名称，使修改后的数据库信息持续 5 分钟绕过裁决。

黑盒方式：直接将拟态环境开放给战队，通过登录界面对系统进行攻击测试。战队通过挖掘出的漏洞，最大化地控制或扰乱执行体运行，最大限度地触发拟态扰动或者拟态逃逸。

判罚规则：攻击效果的判断形式包括有效扰动、无效扰动、逃逸。

（1）有效扰动

添加战队名称需在数据库中呈现，造成一个执行体扰动报警时，判定为有效扰动。例如，“战队 5”将战队名称添加到后勤部门组织架构中，裁决器报警，判定为有效扰动。

（2）无效扰动

除有效扰动外，其它方式导致的扰动无效。例如，直接篡改页面上的静态文件、图标等静态资源视为无效，或者因其它方式触发的裁决器报警，也判定为无效扰动。

（3）逃逸

战队能够同时在所有执行体中添加战队信息，使修改后的数据信息持续（连续 5 分钟）绕过裁决，判定为逃逸。

2 白盒积分争夺赛

2.1 拟态设备

2.2.1 拟态路由器

白盒挑战开始后，参赛战队使用 ssh 远程登录至开放的执行体中（用户名：root，密码：actor2，端口：8899，设备 IP 由组委会指定），并在该执行体上实施攻击。得分方式为：在执行体上增加一条分配给本战队的路由表项，可以获得扰动得分；如果能渗透至其他执行体，并同时在过半数的执行体上增加一条分配给本战队的路由表项，使该表项能够通过路由裁决，就能获得逃逸得分。

分配给每个战队的路由表项如下所示，其中 xx 为战队编号:

目的 IP:　122.122.xx.0/24　下一跳：192.168.1.100

2.2.2 拟态 Web 服务器

赛题描述:

比赛包括白盒注入和安全测试两个阶段。白盒注入阶段，拟态设备将开放其中一路执行体，参赛战队可在该路执行体上注入后门、木马等攻击程序。参赛战队注入完成后，该路执行体将重新被放至拟态设备执行体环境内；安全测试阶段，参赛战队可运用技术手段连接、执行白盒注入阶段注入的攻击程序，并尝试对被注入执行体、其他未被注入执行体甚至整个拟态设备进行攻击。

攻击目标描述:

成功篡改其中一个或多个执行体的主页 index.html，主页篡改成功标准为：战队在 index.html 页面上添加 team+战队编号（比如战队编号为 01 的战队需在 index.html 页面上添加“team01”，即被认为篡改成功）。共计以下 3 种情况能够得分（计分细则详见赛制方案 8.3.2 章节）:

1、成功篡改执行体主页触发裁决器异常：参赛战队成功篡改某个执行体主页，导致裁决器判定不

一致，并形成异常告警。

2、成功篡改执行体主页导致瞬时逃逸：参赛战队成功篡改多个执行体主页，且篡改后主页一致，访问拟态设备主页 index.html 的结果为该参赛战队篡改后结果，即认定拟态设备处于逃逸状态。逃逸状态不能稳定利用，即认定为瞬时逃逸。

3、成功篡改执行体主页导致完全逃逸：参赛战队成功篡改多个执行体主页，且篡改后主页一致，访问拟态设备主页 index.html 的结果为该参赛战队篡改后结果，即认定拟态设备处于逃逸状态。逃逸状态能够稳定利用且持续时长超过 5 分钟，即可认定为完全逃逸。

2.2.3 拟态文件存储

在给参赛队配发的资源中包含访问存储所必需的 client 及各队对应的 cfg 文件，系统为各队分配了文件目录，同时也对访问权限和写入配额进行了限定，这部分内容是由系统的元数据节点（即设备 IP 地址）进行管理维护的。

攻击目标：对于第 *x* 号参赛队，篡改系统中指定的元数据目录/team_*x*/，越权创建文件“MMS_No*x*_FlagInsertion”，突破配额限制写入战队信息内容。

得分判定：(1) 成功在一个在线执行体中达成攻击目标，并通过该目标触发裁决器异常报警，即可扰动得分；

(2) 在首次进行扰动后，系统会进行扰动恢复处理。处理后仍能基于攻击目标产生二次或更多次扰动，则可以追加得分；

(3) 基于攻击目标，使得文件系统的篡改状态能通过外部访问稳定呈现**（持续 3 分钟）**，即可逃逸得分。

注意事项：

(1)扰动/逃逸得分必须成功在其中一个/全部在线执行体中创建指定名称的文件并写入相应内容。凡是没有实现上面目标的扰动属于无效扰动，不会得分。

(2)必须通过攻击拟态设备自身并造成扰动或逃逸才可以得分，通过中间人劫持等只导致客户端回显结果改变的攻击为无效攻击。

(3)参赛战队不允许进行 DDOS 攻击、破坏设备环境等影响其他选手正常比赛的攻击，如被第一次发现，不仅不得分数而且会另外扣除该队 1000 分，并提前结束本轮测试；如被第二次发现，则取消该队比赛资格。

2.2.4 拟态域名服务器

攻击目标：成功修改拟态域名服务器在线执行体对指定域名的解析结果至一个指定 IP 地址。

得分判定：(1) 成功修改其中一个在线执行体对指定域名的解析结果至一个指定 IP 地址，并触发裁决器异常报警，即可扰动得分；

(2) 同时修改全部在线执行体对指定域名的解析结果至一个指定 IP 地址，并使该映射关系持续（连续 5 分钟）通过裁决，即可逃逸得分。

注意事项：(1)扰动/逃逸得分必须成功修改其中一个/全部在线执行体的指定域名的解析结果至一个指定 IP 地址。凡是没有实现上面目标的扰动属于无效扰动，不会得分。 (2)必须通过攻击拟态设备自身并造成扰动或逃逸才可以得分，通过中间人劫持等只导致客户端回显结果改变的攻击为无效攻击。(3)参赛战队不允许进行 DDOS 攻击、虚拟机穿透宿主机等影响其他选手正常比赛的攻击，如被第一次发现，不仅不得分数而且会另外扣除该队 1000 分，并提前结束本轮测试；如被第二次发现，则取消该队对拟态域名服务器的比赛资格。

2.2.5 拟态数据库

注入方式：攻击者通过 ssh 接入开放执行体进行漏洞注入，注入完成后，环境切换至攻击模式，

访问方式：使用附件中提供的驱动程序（示例代码）来连接和访问数据库。攻击者可自行修改示例代码。

攻击目标：创建 teamxxx 命名的账号，并使用 teamxxx 账号创建 teamxxx 名称的数据表。xxx 为分配给战队的 teamid

得分判定：(1)基于攻击目标，触发裁决器异常报警，即可扰动得分；(2)基于攻击目标，查询到指定记录，即可逃逸得分。

注意事项：(1) 扰动得分必须基于攻击目标实现有效的裁决器异常报警，凡是没有基于攻击目标的异常报警，不会得分(2)必须通过攻击拟态设备造成扰动或逃逸才可以得分，通过中间人方式劫持服务显示结果的方式判为无效攻击。

2.2.6 拟态交换机 A

成功配置一条 ACL 规则：an ACL rule was successfully configured

战队编号 X∈（1-48），X 为分配给战队的 teamid

1) 创建 ACL：acl number 200X

2) 设置规则：rule 1 permit 192.168.20.X/0.0.0.0

3) 绑定到端口：traffic limit ingress acl number 200X 1 cir 1000

2.2.7 拟态交换机 B

攻击目标：利用交换机内部漏洞后门窃取交换机内配置文件。

得分判定：

1) 选手使用 tftp 方式将交换机配置文件传输到选手电脑，认定为突破设备得分；

2) 成功突破一个执行体，并开始文件传输，触发裁决器发出对 tftp 的异常报警，认定为扰动得分。

赛题过程:

1) 将 configwbx 用户交给选手，该用户有 operator 权限，允许对执行体进行除删除系统文件之外的其他操作;

2) 选手完成注入后断开与交换机的会话，并通知我方人员;

3) 我方开启拟态模式，修改交换机配置，以此确保选手不能以白盒单执行体状态下拿到的配置文件作为得分依据;

4) 通知选手可以开始窃取动作;

5) 根据选手提交的操作报告和我方设备日志上报，判定选手是否得分。

注意事项:

1) 选手或有其他手段突破交换机的 CLI 界面，将木马埋入子卡，但是在触发木马前需告知我方人员注入完成，并断开会话，我方人员打开拟态模式后，选手再进行窃取动作。

2) 打开拟态模式后，因选手操作所产生的和赛题无关的扰动（非 TFTP 扰动）和清洗不上报日志服务器，且不得分。

2.2.8 拟态云-云平台

注入方式：攻击者通过 ssh 接入开放执行体进行漏洞注入，注入完成后，环境切换至攻击模式，

访问方式：攻击者使用浏览器访问拟态云平台，完成漏洞激活与触发。

得分规则: 成功创建 teamxxx 命名的虚拟机。xxx 为分配给战队的 teamid。

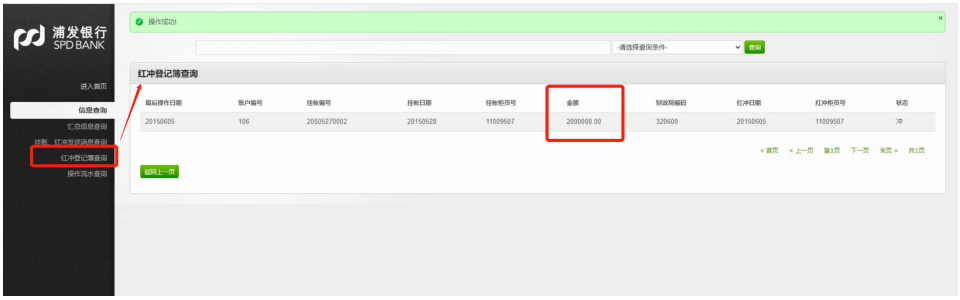
攻击目标：创建 teamxxx 命名的虚拟机得分判定：（1）扰动得分：基于攻击目标，战队将原信息

修改为其它值，并触发裁决器异常报警即可得分，其它扰动报警视为无效。（2）逃逸得分：基于攻击目标，战队篡改的信息能够通过外部访问，且使篡改后的数据信息持续（连续 5 分钟）通过裁决。

注意事项：（1）有效得分：只有通过达成上述攻击目标，并在外部访问触发扰动或逃逸才能得分。（2）无效攻击：篡改页面其它信息造成扰动或逃逸，不得分；通过中间人攻击劫持云应用的服务，并未对防护对象“真正”实施篡改，导致在外部呈现已篡改信息，视为无效行为，不得分；仅篡改执行体内的网页信息，而未对后台数据进行修改，造成扰动不得分。（3）罚分规则：通过关闭/重启云应用服务触发裁决扰动被视为违规，扣除 1000 分，并中止本轮挑战测试。

2.2.9 拟态云-某银行业务系统

攻击目标：银行缴费系统应用预置 1 条“红冲登记”记录信息（金额为 2000000.00，url 为：http://a.b.c.d:e/NTczfs /query/queryGzdjb.action?pageResultSet.pageInfo.currentPage=1），篡改该信息页的登记金额为指定的数值。例如，战队 01 篡改为 2010000.00，战队 48 篡改为 2480000.00。白盒执行体内预先植入了一个 shell，并有两个可用参数，分别为 f 和 t，可以利用这两个参数上传文件。



得分判定：（1）扰动得分：基于攻击目标，战队将金额修改为指定的数值，并触发裁决器异常报警即可得分，其它扰动报警视为无效。（2）逃逸得分：基于攻击目标，战队篡改的记录能够通过外部访问，且使篡改后的数据信息持续（连续 3 分钟）通过裁决。

注意事项：（1）有效得分：只有通过达成上述攻击目标，并在外部访问触发扰动或逃逸才能得分。（2）无效攻击：篡改页面其它信息造成扰动或逃逸，不得分；通过中间人攻击劫持银行缴费应用服务，

并未对防护对象“真正”实施篡改，导致在外部呈现已篡改信息，视为无效行为，不得分；仅篡改执行体内的网页信息，而未对后台数据库进行修改，造成扰动不得分。(3) 罚分规则：通过关闭/重启银行缴费应用触发裁决扰动被视为违规，扣分并中止本轮挑战测试。

2.2.10 拟态云-即时通信系统

本赛题的解题目标为参赛者将战队名称添加到后勤部门组织架构中（篡改本地浏览器 Web 界面的方式无效），触发裁决器异常报警即可得分，其它扰动报警不得分。其中，突破设备逃逸的标准是同时在所有执行体用户 Web 界面后勤部门中添加战队名称，使修改后的数据库信息持续 5 分钟绕过裁决。

白盒方式：直接将白盒执行体开放给战队，通过登录界面对系统进行漏洞挖掘，注入完成后，开放的白盒执行体会引入到拟态系统中，然后切换到拟态业务模式。

判罚规则：攻击效果的判断形式包括有效扰动、无效扰动、逃逸。

（1）有效扰动

添加战队名称需在数据库中呈现，造成一个执行体扰动报警时，判定为有效扰动。例如，“战队 5”将战队名称添加到后勤部门组织架构中，裁决器报警，判定为有效扰动。

（2）无效扰动

除有效扰动外，其它方式导致的扰动无效。例如，直接篡改页面上的静态文件、图标等静态资源视为无效，或者因其它方式触发的裁决器报警，也判定为无效扰动。

（3）逃逸

战队能够同时在所有执行体中添加战队信息，使修改后的数据信息持续（连续 5 分钟）绕过裁决，判定为逃逸。

2.2 ADAS 设备

本次大赛提供商用 ADAS 和拟态 ADAS 设备进行同台竞技，共 16 套设备，通过同类设备的横向对比来检验商用 ADAS 系统和拟态 ADAS 系统各自的安全性。

一、比赛评分规则

本次大赛提供商用 ADAS 系统产品和拟态 ADAS 系统接入比赛，对 ADAS 系统进行漏洞挖掘和拟态防御效果对比。为增加比赛的挑战性和趣味性，将根据评估，选择扰动环节中漏洞危害高和逃逸成功（需描述详细的漏洞发现及触发过程步骤、漏洞利用脚本或程序等）且有意愿参与实车验证的参赛队伍，进行远程实车验证，实车将搭载非拟态 ADAS 系统和拟态 ADAS 系统。对能够通过非拟态系统实际影响车辆的参赛队伍，额外奖励 5000 元，对能够利用拟态系统实际影响车辆的参赛队伍，额外奖励 10000 元。

注意：

- 比赛所用的 ADAS 系统均是市面上主流产品，任何参赛团队不得外泄 ADAS 系统的厂家信息和漏洞信息，否则将承担相关责任；
- 攻击团队漏洞挖掘时不得故意对 ADAS 系统进行不可恢复的攻击行为，否则将扣除大赛总积分的 10%，并提前结束 ADAS 的资格赛比赛；
- ADAS 系统开放接口：CAN 接口，网络接口，USB 调试口；
- 除主办方个别提供的配套软件以外，不允许在跳板机上安装与设备配套的编程调试软件。

商用 ADAS 系统及拟态 ADAS 系统通过跳板机接入，跳板机（共 16 个跳板机）接入大赛系统（大网），跳板机根据参赛队伍需求，可配置 Linux 和 Windows 操作系统，比赛开始后参赛队伍将需要的工具传输到跳板机中，即可开始对接入跳板机的 ADAS 系统进行漏洞挖掘。

Windows：win10 企业版，4GB 内存、4 核，80GB 磁盘空间，2 个网卡，C、D 两个盘符（参赛队伍工具文件请放置在 D 盘中），用户名/密码：test/123456，开放远程桌面。

Linux：ubuntu 20.04、4GB 内存、4 核，80GB 磁盘空间，2 个网卡，用户名/密码：test/123456，

开放 SSH、远程桌面。

1、ADAS 系统申请规则

本届大赛提供市面上主流的 ADAS 系统产品和拟态 ADAS 系统，共 16 套，随机编号为 01、02、03、04、05、06、07、08、……、16，各参赛队伍根据“先到先选”的原则，可在参赛平台上申请未被占用的编号 ADAS 系统进行漏洞挖掘，并在申请时需提供所选择的跳板机操作系统，选中后该 ADAS 系统的有效占用时间为 50 分钟，过时释放，若还需要对该 ADAS 进行漏洞挖掘，将重新排队等待下一次的漏洞挖掘。

2、ADAS 系统计分规则

ADAS 系统的评分标准分为漏洞报告、利用漏洞造成扰动以及拟态逃逸三类评分标准，其中漏洞报告和利用漏洞报告造成扰动两类不重复进行计分，按照最高得分进行计分，拟态逃逸单独计分。所有参赛队伍得分将以漏洞报告为准，未提交漏洞报告或漏洞报告验证无效不得分。

2.1 漏洞报告计分标准

漏洞报告计分标准：参赛队伍挖掘出了 ADAS 漏洞，并需提交挖掘到的漏洞报告（需描述详细的漏洞发现及触发过程步骤），但并未利用漏洞造成 ADAS 系统输出扰动。

级别	漏洞类型	分值
Level3	信息泄露、弱口令，基于原生系统命令导致设备工作异常等漏洞	1000
Level2	基于设备代码健壮性缺陷导致的 DOS 等漏洞	2000
Level1	基于设备代码安全隐患导致的代码执行、远程读写等漏洞	3000

根据漏洞的严重程度，主要分为三级，计分标准如下：

如参赛战队发现疑似但无法利用的漏洞，可提交漏洞报告至裁判组，由裁判组人工评判给予相应

分数，人工审核通过后更新成绩。

漏洞挖掘环节参赛战队可多次提交报告。参赛队伍本轮漏洞挖掘获得的得分，综合计算后计入大赛总积分，参与大赛的奖励评比。

2.2 漏洞扰动计分标准

漏洞扰动计分标准：在 ADAS 标准输出下，参赛队伍通过挖掘利用 ADAS 系统漏洞成功屏蔽或篡改该 ADAS 的感知决策报文则认定为扰动得分，其他扰动不得分，并提交详细的漏洞利用过程报告。

根据漏洞扰动的严重程度，主要分为三级，计分标准如下：

级别	漏洞类型	分值
Level3	信息泄露、弱口令，基于原生系统命令导致设备工作异常等漏洞造成的扰动	2000
Level2	基于设备代码健壮性缺陷导致的 DOS 等漏洞造成的扰动	3000
Level1	基于设备代码安全隐患导致的代码执行、远程读写等漏洞造成的扰动	4000

2.3 拟态逃逸计分标准

计分标准：在 ADAS 标准输出下，屏蔽或篡改拟态 ADAS 系统输出的感知决策报文，并实现裁决逃逸，使该输出报文能够生效，需提供详细的漏洞利用报告。

瞬时逃逸突破：参赛队伍如突破裁决机制造成指定目标的逃逸状态，但并不能稳定利用，控制拟态构造设备修改其中的指定目标数据。

完全逃逸突破：队伍如完全突破裁决机制造成指定目标的完全逃逸状态，控制拟态构造设备修改其中的指定目标数据，可稳定利用且逃逸时长超过 5 分钟。

瞬时逃逸情况下，各参与攻击拟态 ADAS 的参赛队伍将平分 10000 分。

完全逃逸情况下，各参与攻击拟态 ADAS 的参赛队伍将平分 20000 分。

注意事项：(1) 扰动/逃逸得分必须成功在其中一个/全部在线执行体输出报文中修改为指定给本战队 ADAS 自身的报文。凡是没有实现上面目标的扰动属于无效扰动，不会得分。输出报文修改为指定给其他战队的 ADAS 报文不得分。(2) 必须通过攻击拟态设备自身并造成扰动或逃逸才可以得分，通过中间人劫持等只导致回显结果改变的攻击为无效攻击。

3、ADAS 系统漏洞实车验证

为增加比赛的挑战性和趣味性，本届大赛新增实车验证环节，实车验证时间安排在 2021 年 11 月 12 日 9:00-12:00。实车将搭载非拟态 ADAS 系统和拟态 ADAS 系统。主办方将根据评估，选择扰动环节中漏洞危害高和逃逸成功（需描述详细的漏洞发现及触发过程步骤、漏洞利用脚本或程序等）且有意愿参与实车验证的参赛队伍，每支队伍有效验证时间为 1 小时，进行远程实车验证，对能够通过非拟态系统实际影响车辆的参赛队伍，额外奖励 5000 元，对能够利用拟态系统实际影响车辆的参赛队伍，额外奖励 10000 元。

ADAS 漏洞报告

参赛队伍：

报告时间：

漏洞名称	
漏洞效果	

（利用）	
漏洞发现及触发步骤（详细描述）	
其他（攻击程序、脚本等附件的链接）	

附件 4、拟态防御参考书

中文版京东：

https://search.jd.com/Search?keyword=%E7%BD%91%E7%BB%9C%E7%A9%BA%E9%97%B4%E6%8B%9F%E6%80%81%E9%98%B2%E5%BE%A1%E5%8E%9F%E7%90%86&enc=utf-8&wq=%E7%BD%91%E7%BB%9C%E7%A9%BA%E9%97%B4%E6%8B%9F%E6%80%81%E9%98%B2%E5%BE%A1%E5%8E%9F%E7%90%86&pvid=c009a1f75fd944d59c15b26b217b13df

中文版当当：

http://search.dangdang.com/?key=%CD%F8%C2%E7%BF%D5%BC%E4%C4%E2%CC%AC%B7%C0%D3%F9%D4%AD%C0%ED&act=input

中英文版亚马逊：

https://www.amazon.com/-/zh/dp/3030298434/ref=sr_1_1?__mk_zh_CN=%E4%BA%9A%E9%A9%AC%E9%80%8A%E7%BD%91%E7%AB%99&dchild=1&keywords=mimic+defense&qid=1589218017&sr=8-1

英文版 Springer:

https://www.springer.com/cn/book/9783030298432?from=timeline&isappinstalled=0#bibliographic

英文版京东：

https://item.jd.com/64536793597.html

附件 5、拟态防御基准功能实验

请见 PDF 文件《Mimic Defense Benchmark Function Experiment》

赛宁网安