DEFCON 中国赛技术方案（草案）

1. 背景

2018 年，世界上网络安全最高级别盛会 DEFCON 正式登陆中国，与百度安全联合主办“御 • 见未来”2018 首届 DCCB（Def Con China Baidu）安全行业国际峰会。作为此次峰会的重要组成部分，受百度公司委托，永信至诚公司承办，依托“e 春秋网络安全实验室-靶场竞赛平台”在本次峰会期间将举办为期一天半的网络安全竞赛。

2. 竞赛时间

线上预选赛：2018 年 4 月 21 日 8:00 ～ 2018 年 4 月 21 日 17:00

线下总决赛：2018 年 5 月 11 日 12:00 ～ 5 月 12 日 17:00 (11 日晚人类队伍离开场地)

网友嘉年华-众测彩蛋：2018 年 5 月 12 日 9:00～15:00

战队报名时间时间：2018 年 4 月 2 日 00:00 ～ 2018 年 4 月 13 日 24:00

3. 赛制及规则

3.1. 参赛队伍

- 竞赛采用线上预选赛、线下总决赛两级赛制。
- 线上预选赛采用社会组团报名制，所有队伍人数不限，但最终上场队员不得超过八名，其中一人为队长。报名网址暂定为：defcon-ctf.ichunqiu.com
- 线下总决赛采取邀请制，共十六只队伍参赛，队伍人数不限，但最终入场队员不得超过八名，其中一人为队长。
- 决赛队伍来源及方式：
  - 邀请十只国际及国内具有 defcon 参赛水平的高水平战队、三只国内高水平的 AI 程序战队参加线下决赛，线上预选赛的前三名也将获得资格参加线下总决赛。

3.2. 线上预选赛

- 线上预选赛采取传统的 ctf 解题方式，赛题涵盖 web、pwn、crypt、misc 等，赛题难度与常规 BCTF 相当。

赛题总数设置为 10 道，保持 pwn 和逆向等题目比例占 70%左右，增加 AI 方向题目，具体题目比例如下表

原则上，指令集，操作系统，漏洞类型等全部不限。

3.3. 线下总决赛

线下总决赛分为 AI 程序漏洞攻防挑战赛、靶场渗透及 CTF 攻防对抗赛两项赛事。

两项赛事同时进行，每个战队将通过统一的战队接口接入两个赛场同时进行角逐，综合考察每个参赛队伍在自动化攻防、CTF 攻防对抗以及内网综合渗透等各方面的对抗能力。

3.3.1. AI 漏洞攻防挑战赛

本项比赛侧重考察各战队的 AI 程序在无人类干预情况下或人类在自动化工具辅助下针对 linux32 位程序的漏洞发现、挖掘、和利用能力，为了鼓励纯自动化和 AI 发展，对纯 AI 程序参赛的队伍设立单独奖项。

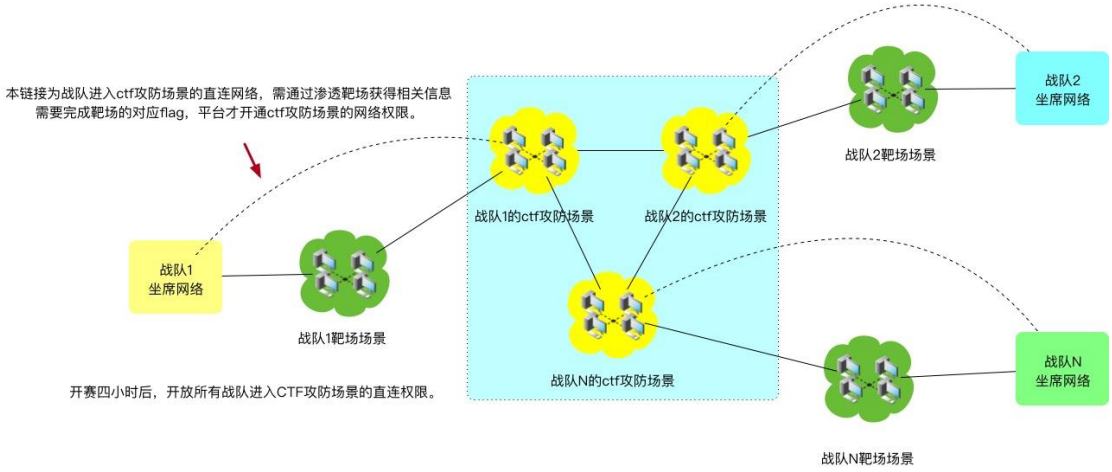
- **赛题**：采用标准的 linux32 位二进制程序，在平台端运行相应的服务，并在特定端口开放该服务。AI 程序程序通过标准接口与平台交互，并下载统一格式的接口文件，获知二进制文件的下载地址、对应赛题运行的 IP 和端口号，以及 flag 文件的存储地址、flag 提交接口等。AI 程序在本地分析二进制赛题，并生成利用程序对目标赛题发起攻击，通过控制目标赛题的进程读取 flag 值，并向特定地址进行 flag 提交得分。
- **奖项**：本项赛事的积分将统一计入赛事总积分，本单项赛允许纯 AI 程序参赛，也允许其他人类战队参赛，但仅纯 AI 程序参赛的队伍将单独参评“AI 漏洞挑战赛优胜奖”或“最佳漏洞挖掘 AI 奖”，人类战队参赛将获得积分。
- **积分规则**：每道赛题的初始分均为 128 分，共计 50 道题目，比赛开始后同时放出。任意一道赛题，第一个提交正确 flag 的战队得 128 分，第二名提交者得 64 分，第三名得 32 分，以此类推，从第八名开始都仅得 1 分。本项比赛不设轮次。
- **算力要求**：针对纯 AI 程序参赛的战队，本项赛事设定标准的 AI 程序算力环境要求，算力环境服务器由赛事主办方统一提供，暂定为两颗 8 核 16 线程 cpu，128G 内存和 6TB 硬盘（算力环境会影响 AI 程序的效率 ，

有战队要求 2 颗 64 核 CPU 和 512G 内存）。

- **纯 AI 程序隔离**：报名纯 AI 程序参赛的战队，需在赛前 3 天完成与竞赛平台的联调。比赛开始后，参赛 AI 程序将不允许任何人为的干预和调整。运行 AI 程序的服务器将放置在指定位置，人类或战队不得再进行干预。
- **积分比例**：本项比赛积分占总积分比例为 20%。
- **特点**：本赛区赛题采赛题数量较大、赛题相对简单的漏洞题目，有利于发挥出 AI 程序快速解决较简单漏洞的特点，本次赛制比 rhg2017 更进一步 ，实战性更强，直接针对漏洞进行利用并执行系统命令。

3.3.2. 靶场综合渗透及 CTF 攻防对抗赛

本项比赛侧重考察各战队的靶场综合渗透能力和 CTF 攻坚能力。靶场综合渗透利用多个虚拟节点构建一个仿真靶场网络，考察队伍的漏洞利用、单机渗透、内网渗透等技能；CTF 攻防对抗赛的赛题形式和难度与历届 defcon CTF 竞赛相当，各战队对自己防御区域内的赛题进行漏洞挖掘和防御，同时对其他战队的防御赛题进行攻击，获取 flag 得分，被夺取 flag 的队伍被扣分。



- **赛制：**
  - 比赛平台为每个战队准备独立但完全一致的靶场环境，考察战队的综合渗透能力。比赛开始，各个参赛队伍将得到该靶场入口信息，战队须通过不断的进行渗透寻找线索来逐步深入。
  - 靶场赛中战队通过渗透通关后，得到并提交特定的 flag，平台将自动开通该战队进入 CTF 对抗赛的网络权限，并通知该战队其防守 gamebox 的 ip 和防御账号。则该战队可进入 CTF 对抗赛区域进行攻防。先进入 CTF 对抗赛去的队伍将抢得先机。
  - 统一权限开启开关：比赛开始 4 个小时后（或依据现场情况决定），同时开启所有战队的 CTF 对抗赛接入权限，并同步各队伍账号。CTF 对抗赛开始（其体验与传统 DEFCON 对抗赛一致）

- **靶场赛题：**在保证难度的情况下，保证半数左右战队可以在 4 个小时左右拿到权限。拟设定 12 个虚拟节点，4 个安全大区组成的虚拟靶场场景作为赛题，考察队伍的连续综合渗透能力和数据获取和分析能力。
- **CTF 对抗赛题：**采用与传统 DEFCON 攻防决赛相同类型和难度的赛题。按正式比赛时间 14 小时计算（比赛当晚清场），本项比赛共设约 5 道赛题，平均每个赛题 5 个漏洞点左右。
- **积分规则：**
  - 为让现场观众能够知晓战队进展，靶场赛题中也需设置 flag，战队通过提交 flag 取得相应积分。本部分积分占总积分 20%左右，其中打开 CTF 对抗赛区域网络权限的终极 flag 占总积分的 10%。
  - CTF 对抗赛题采用与传统 DEFCON 决赛相当的零和积分方式，每个队伍拥有三道赛题的运行环境，队伍需要通过分析赛题发现漏洞，完成漏洞利用程序和补丁程序，一方面防御自己的赛题不失分，另一方面通过攻击其他参赛队伍赛题得分。参赛队伍须保证己方赛题正常提供服务，赛题异常的队伍在本轮会进行扣分，扣掉的分数会平均分配给本轮所有该道赛题正常的队伍。为保障中国赛和传统 DEFCON 的沿袭，本项比赛积分占总积分比例不低于 60%。
- **轮次：**每十分钟一轮，轮次结束时统计各参赛队在本轮的得分。

3.3.3. 网友嘉年华-众测彩蛋

本项比赛旨在推动广大网友同步参与 defcon 中国总决赛，因此在 5 月 12 日总决赛正赛期间，在比赛现场放置若干智能设备进行众测，发现这些设备漏洞并证明该漏洞风险的队伍，经过厂家裁判团队的评判确认，可获得相应的彩蛋奖励。