XXXXXXXXXXX

参赛须知

Entry information

- **赛事概述 Event Description**

- 赛事概述 **Event Description**

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。

In 2018, DEFCON, which enjoys the world's highest level of cybersecurity event, officially landed in China .With the Cooperation of Baidu Security, the first **“YU·JianWeiLai”** DCCB(DefCon China Baidu) will be held in China. As a significant part of the DefCon meeting, the DCCB uses the "eChunQiu Cyber Security Lab-Cyber Range Platform" as the environment and will last for a day and a half, will be undertaken by Intergitytech and entrusted by Baidu.

- 赛事特点 Event Features
- 竞赛形式 Event Category

• 赛事细则 Event Details

- 竞赛时间 Competition Time
- 流程介绍 Schedule introduction

本次赛事由三场竞赛组成，分别为人工智能赛（RHG）、靶场赛（CR）和攻防赛（AWD）。

The competition consists of three parts, RHG (Robot Hacking Game), CR (Cyber Range game) and AWD(Attack with Defense).

其中人工智能赛和靶场赛开始时间与本次赛事开始时间相同；攻防赛会在参赛队获取靶场赛通关权限后开启，同时在本次赛事开场 4 小时后，所有参赛队均可获得参与攻防赛的资格。

RHG and CR will begin simultaneously as the competition begins, and your team can join the AWD when you finish the CR. 4 hours after CR begins, all team can join the AWD.

- 人工智能赛细则 RHG Rules

- **赛制描述 Rules Description**

本场竞赛开始时间与本次赛事开始时间相同，无准入门槛。

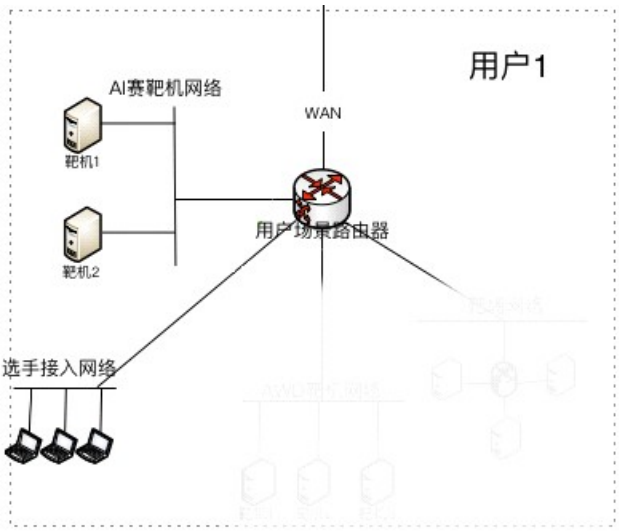
The RHG starts at the beginning of the competition. Every team can join in unconditionally.

在本场的竞赛中，参赛队使用自行研发的机器人参与竞赛，或以人类身份参与竞赛。每支队伍配备 50 道题目，每道题目具体得分规则请参考“评分规则”。

Your team can use your own AI robot to solve challenges or solve challenges by yourselves. We have prepared 50 challenges for each team. Please refer to “Scoring Rules” for specific scoring rules for each challenge.

本场竞赛中，参赛队（机器人或人类）与题目的拓扑关系如下图所示：

The relationship of team and challenge server is shown in the picture below:



本场竞赛中的每道赛题均包含一个漏洞，漏洞类型包括所有的内存访问异常类漏洞，出现在题目中的内存访问异常类漏洞包括但不限于栈溢出、堆溢出和格式字符串漏洞等。

Each challenge contains a vulnerability to attack, which include but are not limited to stack overflows, heap overflows, and format string vulnerabilities.

本场竞赛的赛题具有如下特性：

Challenge Features:

- 32 位 Linux 二进制程序
- 32-bit Linux program
- 静态编译
- Static compilation
- 堆栈保护关闭、无地址空间随机
- NO DEP，NO ASLR
- gcc 编译（版本 TBA）
- gcc
- 单进程，单线程
- Single process，Single Thread

所有的赛题均设计为从标准输入接收输入数据，并将结果发往标准输出（网络服务通过管道网络连接标准输入输出）。

All challenges are designed to receive input data from standard input and send results to standard output（Network services connect standard input and output via pipeline network）

具体运行环境如下：

runtime environment

- [Ubuntu 16.04.4 Server (32-bit)]
- [内核版本: 4.4.0-116-generic]
- [GDB 版本: 7.11.1]
- [GCC 版本: 5.4.0 20160609]
- [glibc 版本: 2.23]
- [ASLR 关闭]
- [DEP 关闭]

• 答题方式 How to Submit flag

若作为机器人参赛，系统为机器人提供了自动答题接口，地址如下：

if your team wants to use robots to submit flag, we have provided the api below:

http://172.16.4.110/api/sub_answer

如上地址使用示例如下：

For example:

```
curl -d "answer=xxx" -X POST -v --user user:pwd

http://172.16.4.110/api/sub_answer
```

若作为人类参赛，通过各种攻防手段获取 Flag 后，可在 https://172.16.4.1 页面上进行登录，并在答题框中输入 Flag，即可得分。登录所需用户名和密码请参见密码信封。

if your team wants to submit flag by yourselves, you can login in https://172.16.4.1 with the username and password in the secret envelope, and submit the flag in the Input box.

flag 存放位置 where to put the flag

每道赛题 flag 位置为：/home/flag 题目编号.txt

The flag of each challenge storage at： /home/flag(challengeID).txt

例如：

For example

若题目编号为 1，flag 文件为/home/flag1.txt

If challenge ID is 1, then flag is /home/flag1.txt

若题目编号为 10，flag 文件为/home/flag10.txt

Challenge ID is 10, flag is /home/flag10.txt

- 靶场赛细则 CR Rules

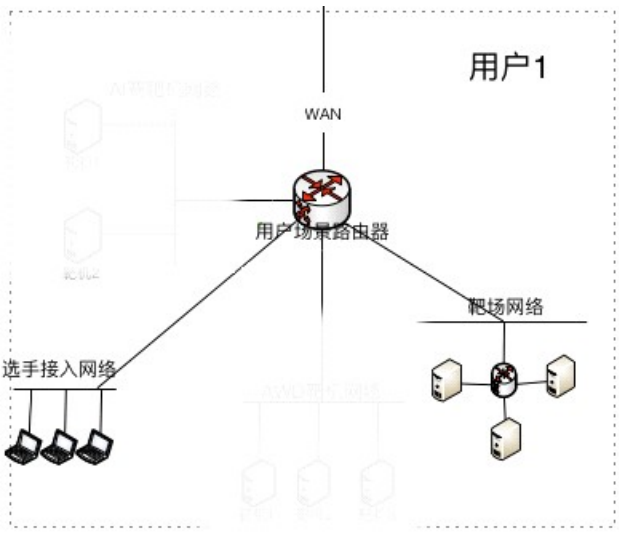
- **赛制描述 Rules Description**

本场竞赛开始时间与本次赛事开始时间相同，无准入门槛。

The CR start at the beginning of the competition. Every team can join in unconditionally.

在本场的竞赛中，每支参赛队将会进入到仿真网络靶场中进行角逐。每支参赛队将都会被分配一个独立、完整、相同的仿真网络场景，此网络场景与参赛队的网络拓扑关系如下图所示：

Each team will enter the virtual network environment to do penetration test. The environment for each team is the same, independent and complete. The network structure is shown in the picture below:



上图中所示的靶场网络内的网络结构为示意图，为了让竞赛更具挑战性，参赛队需要自行发觉靶场网络内的真实网络结构。

The picture is just an example. Your team have to find the true network structure by yourselves.

在本场竞赛所构造的场景中，共包含 10 个关键节点，在此 10 个关键节点中，共藏匿了 6 个 flag，每个 flag 所对应的分值各有不同，具体分值请参见下表：

In the CR, there are 10 Key nodes. You can get all flags (6 flags) in the virtual network environment. Each flag has a different score as the following form shows:

题目序号及对应的分值(challenge Id and It's score)		
Flag 名称(flag id)	**Flag 类型(flag type)**	**分值(score)**
Flag 1	基本 Flag(basic)	1000
Flag 2	基本 Flag	1000
Flag 3	基本 Flag	1200
Flag 4	基本 Flag	1200
Flag 5	基本 Flag	1400

Flag 6	核心 Flag(core)	1800

在本场的竞赛中，获取 3 个基本 Flag 以及 1 个核心 Flag 即可通关，并开启进入攻防赛的权限。通关后，本场竞赛还可继续答题得分。

You can join the AWD if you get 3 basic flag and 1 core flag. When you start AWD, you can also continue to solve the RC challenges.

- **答题方式 How to Submit flag**

通过攻防手段获取 Flag 后，可在 https://172.16.4.1 页面上进行登录，并在答题框中输入 Flag，即可得分。登录所需用户名和密码请参见密码信封。

you can login in https://172.16.4.1 with the username and password in the secret envelope, and submit the flag in the Input box.

- **flag 存放位置 where flag is**

在本场的竞赛中，Flag 字符串通常存放于名为“flag”的文件中，该文件的存放位置需要参赛队自行寻找。

In RC, flag strings are usually stored in a file named "flag". You must find the file by yourselves.

- 攻防赛细则 AWD Rules

- **赛制描述 Rules Description**

参与本场竞赛需要获取靶场赛通关权限后才有资格参与，同时，大赛开始

4 个小时后，会统一开放参与权限，所有参赛队均可参与本场竞赛。

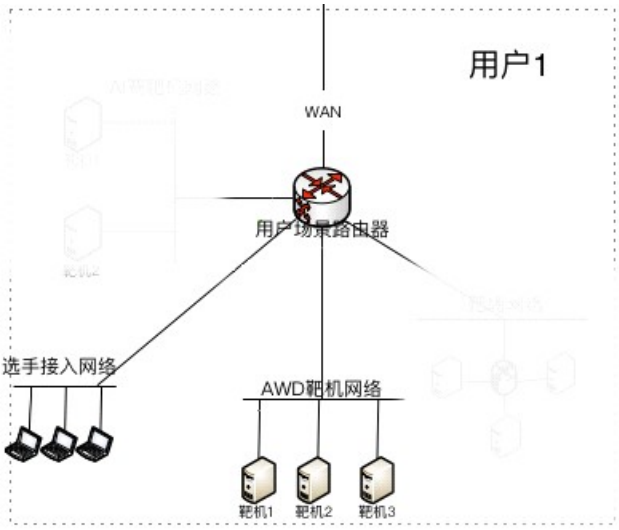
Your team can join the AWD after you finish the CR (after getting 3 basic flag and 1 core flag). 4 hours after the CR beginning, all team can join in the AWD.

在本场的竞赛中，每支参赛队被分配了 4 台 GameBox。每台 GameBox 上面均存在若干漏洞，在竞赛过程中，参赛队既需要防护己方 GameBox 免受攻击，又需要攻击其他参赛队的 GameBox 从而获取得分。

Each team has 4 GameBoxes. There are several vulnerabilities in each GameBox. During the competition, you need to protect your own GameBox from attack, and also need to attack GameBox of other teams to get points.

每个 GameBox 与参赛队的网络拓扑关系如下图所示：

The Network structure is shown in the picture below:



本场竞赛所准备的 4 台 GameBox 信息如下表(表在哪儿？)所示，维护各 GameBox 所需用户名和密码请参见密码信封。

The information of 4 GameBox is shown in the table below. The username and password required to operate and maintain each GameBox are in the secret envelopes.

• 答题方式 How to Submit flag

通过攻防手段获取 Flag 后，可在 https://172.16.4.1 页面上进行登录，并在答题框中输入 Flag，即可得分。登录所需用户名和密码请参见密码信封。

you can login in https://172.16.4.1 with the username and password in the secret envelope, and submit the flag in the Input box.

同时，在本阶段的竞赛中，系统提供了自动答题接口，参赛队可通过撰写脚本进行自动答题，自动答题接口如下所示：

we also provide an API for your automatic submission as the following:

https://172.16.4.1/Common/awd_sub_answer

本接口需要通过 **POST** 方式提交，提交时所需携带参数如下表所示：

You need to post the flag with the format in the following table:

自动提交接口参数描述(parameter description)	
参数名(parameter name)	**值(value)**
answer	获取的 flag(the flag you get)
token	请参见密码信封(in secret envelope)

- **flag 存放位置 Where to put The Flag**

在本场的竞赛中，Flag 字符串通常存放于名为“flag”的文件内，该文件通常位于各 GameBox 的根目录下，并每轮更新一次。

In AWD, flag strings are usually stored in a file named "flag" at the Root directory. it will be updated for each round.

• 评分规则　Scoring Rules

• 总分计算方法 Total Scoring Rules

The total score of this competition will be the sum of scores of RHG, CR, AWD. The proportion of each competition is shown in the following table:

总分组成方式(proportion of each competition)		
人工智能赛（RHG）	靶场赛（CR）	攻防赛（AWD）
20%	20%	60%

• 人工智能赛计分规则 RHG Scoring Rules

本场竞赛的评分规则为，按照解题速度排名评分，针对于每个题目，第一名解答的队伍将会获得满分，后面答对的题目得分依次递减，详情如下表所示：

The scoring rules for this competition is as follows:

Scoring will be determined according to the speed of problem solving. For each challenge, the team solve the challenge first will get full marks, and the scores of the challenge that are solved later will be reduced in turn. The details are shown in the following table:

得分详情(scoring details)	
解题名次(ranking)	得分(score)
第 1 名	128
第 2 名	64
第 3 名	32
第 4 名	16
第 5 名	8
第 6 名	4
第 7 名	2
第 8 名	1
第 9 名	1
第 10 名	1
第 11 名	1
第 12 名	1
第 13 名	1
第 14 名	1
第 15 名	1
第 16 名	1

- 靶场赛计分规则 CR Scoring Rules

本场竞赛的评分规则为，答对相应题目即可获得相应分数，每题分数如下表所示：

you can get the scores when you get the flag. The score of each flag is

shown in the following table.

题目序号及对应的分值(challenge Id and It's score)		
Flag 名称(id)	**Flag 类型(type)**	**分值(score)**
Flag 1	基本 Flag(basic)	1000
Flag 2	基本 Flag	1000
Flag 3	基本 Flag	1200
Flag 4	基本 Flag	1200
Flag 5	基本 Flag	1400
Flag 6	核心 Flag(core)	1800

- 攻防赛计分规则 AWD Scoring Rules

本场竞赛的评分规则为零和计分规则。

AWD is a zero-sum credit game.

在同一轮中，每队的每个 GameBox 被攻克会被扣除 16 分，扣除的分数会被平均分配给成功攻克此 GameBox 的队伍。

In a round, 16 points will be deducted of your team for each GameBox that has been attacked, and the deducted points will be evenly distributed to the team that successfully attack your GameBox.

在同一轮中，每队的每个 GameBox 被 Check 认定为宕机会被扣除 16 分，扣除的分数会被平均分配给次轮中保持此 GameBox 状态正常的团队。

In a round, 16 points will be deducted of your team for each GameBox that is running abnormally judged by Checker, and the deducted points will be evenly distributed to the team in the next round that keep the GameBox running normally.

每队的每个 GameBox 的分数池为 1600 分，此分数若被扣除完毕，则无论发生攻克还是宕机情形，均不会再次失分，同时也不会再有队伍获得分数。

Each GameBox has only 1600 points. If this score has been deducted to 0, no points will be lost even if being attacked or running abnormally. At the same time, no teams will score points through this GameBox.

- 排名方法 ranking rules

本次赛事按照赛事只设定一个排行榜，排行榜按照总分排名，若总分相同则按照最后答题时间排行，最后答题时间越早，名次越靠前。

Only one ranking is set according to the competition rules, and the rankings are set according to the total scores. If the scores are the same, the ranking is based on the last time when you submit flags. The earlier you submit the flag, the higher ranking you will get.

• 竞赛守则 Competition Rules

- 竞赛期间，参赛队需使用合法的用户名、密码登录竞赛平台，若发现人与账号不匹配、账号外借等情况，视情况严重程度，将进行警告、取消参赛资格等处罚措施。
- During the competition, each team must use a valid username and password to log in the competition platform. If the team and the account

does not match or the account is borrowed, etc., depending on the severity of the situation, we will perform warnings, disqualifications, and other penalties.

- 竞赛过程中严禁参赛队伍向竞赛服务器、参赛队伍主机等设施发起任何可能影响竞赛正常运行的渗透或恶意操作，视情况严重程度，将进行警告、取消参赛资格等处罚措施。
- During the competition, it is not allowed to attack the competition infrastructure. Depending on the severity of the situation, we will perform warnings, disqualifications, and other penalties.
- 竞赛期间，禁止参赛选手在互联网上（例如：QQ 群、微信、技术交流论坛等）发布、传播竞赛真题进行求助，若竞赛委员会在网络巡检中发现该类情况，则直接取消该队伍或选手的参赛资格。
- During the competition, it is not allowed to publish and disseminate challenge on the Internet (for example: QQ Group, WeChat, and technical BBS) for assistance. If the referee finds such circumstances during the network inspection, the qualification of players or teams will be directly cancelled.
- 参赛队伍在竞赛期间需遵循裁判及现场工作人员的安排，如有疑问请举手示意。
- You must comply with the arrangements of referees during the competition. If you have any questions, please raise your hand.
- 参赛队伍未经裁判同意，禁止进入他人赛位，干扰其他队伍竞赛。

- You are not allowed to enter other players' positions without the approval of the referees, or interfere with other team.
- 遵守竞赛纪律，切勿喧哗，服从裁判，不得对他人进行语言或人身攻击。
- You should obey the rules of competition and referees. No language or personal attacks on others is allowed.
- 违反上述规定者，现场裁判组将视情况给予口头警告、扣分、取消参赛资格等处罚。
- If you are in violation of the above rules, depending on the severity of the situation, we will perform warnings, disqualifications, and other penalties.